Tiger Team

July 13, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody. Welcome to the Privacy & Security Tiger Team call. This is a federal advisory call, so there will be opportunity at the close of the meeting for the public to make comments, and workgroup members, please remember to identify yourselves. Let me do a quick roll call. Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – eScription – CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Gayle Harrell? Dr. Harrell is representing her momentarily. Latanya Sweeney? Carol Diamond? Judy Faulkner is going to be late, but Carl Dvorak, are you on?

Carl Dvorak – Epic Systems – EVP
I am on.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Dave McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Christine Bechtel couldn't make it together. John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm on.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Leslie Francis? Joy Pritts?

Joy Pritts – ONC – Chief Privacy Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene? Joy Keeler? Did I leave anybody off? All right. Thank you. I'll turn it over to Deven and Paul Egerman.

Paul Egerman – eScription – CEO
This is Paul Egerman. Good morning and thank you for attending our tiger team meeting this morning. I guess there is a distraction at this point right now at 10:00. There is a press conference with apparently the results of meaningful use and certification being announced. So I'm always impressed when Judy Sparrow does a roll call. I'm impressed with everybody's dedication to attend these meetings … impressed today, so thank you very much for attending.

To briefly remind everybody, the tiger team that was organized over the summer to address specific privacy and security issues that have been raised by ONC and to provide practical guidance on health information exchange. And so just for a fixed period of time, we are meeting with a very aggressive schedule. We're meeting twice a week, and the meetings are for about three hours. For the members of the public who are listening to our call, I want to thank you for participating, and also tell you that we do have time at the end of the call for public comments, and that I would encourage you to make comments. We are very interested in the feedback, good, bad, or neutral that you have on what we're doing.

What we are doing right now is we are addressing a series of questions related to data collection and use and reuse, and we had an agenda last week, and we managed to get through three of the six questions, and so I'm going to advance the slides to the four question, so we answered three of the nine questions or six questions remaining. What we would like to do on this call is complete the remaining six questions. If we complete the remaining six questions, in addition to feeling really good, what we would like to do is actually start talking about the consent issues. These questions relating to collection, use, and disclosure of PHI by providers are all extremely interesting questions. When we get to consent, we are also dealing with issues that are extremely interesting. So we think that will be a very exciting discussion.

The first question we want to talk about this morning is a question that is actually question number four, and it is, how should public health reporting be handled? Because we ran a little behind on the agenda, I asked people to think about this question in advance of the call, and to consider that issue in advance of the call. There were a number of e-mails that went back and forth, which were extremely helpful in terms of how public health reporting currently works and what should be the obligations to do reporting. Basically public health reporting is an example of….

Deven McGraw - Center for Democracy & Technology – Director
Paul?

Paul Egerman – eScription – CEO
Yes.

Deven McGraw - Center for Democracy & Technology – Director
You're just breaking up a little bit.

Paul Egerman – eScription – CEO
Okay.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think everybody is breaking up. When you spoke too, it was breaking up as well, Deven.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm experiencing what Deven is experiencing. Paul is breaking up quite a bit, Deven and the other speaker just now were fine.

Paul Egerman – eScription – CEO
Am I still breaking up?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It's a little better.

Deven McGraw - Center for Democracy & Technology – Director
It's better.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
There's an echo on my line, by the way.

Deven McGraw - Center for Democracy & Technology – Director
Did you mute your computer?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It was actually turned off, but I'll try it again. Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
The software actually does permit muting the value output now. It's a welcome change.

Paul Egerman – eScription – CEO
Yes. If you can hear me now, the question number four is how should public health reporting be handled. This is a question, actually I got curious about, so I look at our state, Massachusetts' state public health reporting requirements. And it's a fascinating thing. There's like 100, over 100 different diseases, and the requirement is actually complicated, but there are things like say reporting of tuberculosis where you have to report the PHI and where the state will actually assign a caseworker to follow what's going on with the patient or reporting of West Nile Virus where the state wants to interview the patient to find out what was the source of the disease in order to prevent the spread of infection. Then there's a whole series of other infectious diseases and sexually transmitted diseases.

Looking at it, I can understand why compliance among physicians can sometimes be low because it's complicated to know when you report identification material and when you don't report it. It is the sort of thing that a computer could help considerably with. Now we posed this question, how should public health reporting be handled? Deven, last night, sent out a suggested proposal based on everybody's comments. I don't know if you have it in front of you, Deven, if you would like to review that with people.

Deven McGraw - Center for Democracy & Technology – Director
I will, but can I do the one that Wes modified because it was so much better?

Paul Egerman – eScription – CEO
Absolutely. Let's do Wes' one because it was – actually, if I did it, and I spoke up, if I did the long one, and I broke it up, it'd probably be the same number of words as Wes', but why don't you do Wes'?

Deven McGraw - Center for Democracy & Technology – Director
Sure. It was an attempt to sort of pull into one set of recommendations the comments that folks had chimed in with over e-mail. Public health reporting by providers or HIOs who are acting on their behalf should take place using the least amount of identifiable data necessary to fulfill the lawful public health purpose for which the information is sought. In cases where the law requires the reporting of identifiable data or where identifiable data is needed to accomplish the lawful public health purpose for which the information is being sought, identifiable data may be sent. Consistent with our earlier recommendation, the provider is responsible for disclosures from his or her record, but may delegate lawful public health reporting to an HIO pursuant to a business associate agreement to perform this function on his or her behalf, and such delegation may be on a per request basis or may be a more general delegation to respond to all lawful public health requests. These recommendations are prepared pursuant to the nationwide framework, those fair information practices, as articulated by ONC, in that nationwide framework document of principles and also adopted by the health IT policy committee as part of the strategic plan white paper, and is also consistent with the HIPAA minimum necessary standards.

Paul Egerman – eScription – CEO
There are still a lot of words, but the basic recommendation is to comply with HIPAA, but that physicians can basically delegate either automatic disclosure to an HIE, HIO, if the HIO can do it, or alternatively can delegate, ask the HIO to do the disclosure under a specific set of circumstances. We gave providers two choices, as long as they comply with everything else. Is that a fair summary, Deven?

Deven McGraw - Center for Democracy & Technology – Director
That's right, and it also puts in principles of collection limitation where identifiable data isn't either needed or specified. It should be limited in its identifiabilty when it's provided.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Can you put it up so that we can read it?

Deven McGraw - Center for Democracy & Technology – Director
Yes. Is Linda Kunts on the line?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Deven actually circulated that yesterday.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. I can't find it.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It's actually under Deven's e-mail from Wes, so if you're looking under Wes, it doesn't show up.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I see.

Deven McGraw - Center for Democracy & Technology – Director
Alison, do you have? I sent that to you as well.

Alison Gary – Altarum Institute – Communication Technologies Coordinator
Deven, I do have it in e-mail. I'm offline of my e-mail since I'm broadcasting. I can pass the presentation control back and copy and paste, and massage this data, and then broadcast again. In the interest of saving time, I can just make sure it's incorporated into the deck, and if this is the recommendation, we can move on.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I just wanted people to be able to see it, like we did with folks for the last call.

Alison Gary – Altarum Institute – Communication Technologies Coordinator
I can't broadcast all of my e-mail.

W
Why don't you send it back to …?

Paul Egerman – eScription – CEO
Deven, why don't you send it to her, and maybe …?

Deven McGraw - Center for Democracy & Technology – Director
I'll send it to everybody.

Paul Egerman – eScription – CEO
Yes.

Alison Gary – Altarum Institute – Communication Technologies Coordinator
Deven, this is Alison from Altarum. If you send it to me, I can put it in the downloads pod so that people can retrieve it from there.

Deven McGraw - Center for Democracy & Technology – Director
Great. I'll do that. I'll send it to everybody.

Paul Egerman – eScription – CEO
Everyone wants to look at the actual wording, but as I say, the concept is to comply with the HIPAA sort of—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. In reading through all this yesterday, I had one comment about this, and I'm not sure whether it practically will ever occur, but let me bring the scenario up. What happens if, because this HIO has a lot of information from a lot of different providers, what happens in the event that it is, as a business associate, performing the mandatory reporting or the permissive reporting on behalf of one provider, but ends up using data that has been collected by another provider, and that other provider is doing its own reporting and has not authorized the HIO to do the reporting on its behalf. I'm not sure how that would be handled, if that would be an issue.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
This is Carol. Sorry I joined a few minutes late. I've been actually wondering the same thing, and not necessarily exactly down that path, but on that road anyway, and one suggestion I have is that we're

careful not to imply that even if the HIO is performing the function on behalf of the provider, that the HIO actually needs to collect and retain that data. It's not necessary. I mean, if the HIO is acting as a pass through, it doesn't necessarily need to collection and retain the information that it's passing to a public health authority, even with a business associate agreement.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I guess I'm wondering. I think of this as a service that might be provided on behalf, the value of the service. One scenario is sort of the classic, we're seeing a stream of lab results, and some of them are reportable. Let's send them on to the health association. There are other kinds of reportable information, and there are organizations for HIOs that include repositories. Are we meaning to extend this from they needn't retain to they shouldn't retain, or is it really meant just to say that they needn't retain?

Paul Egerman – eScription – CEO
This is Paul. First, I'd like to ask team members, when you speak, be sure to identify yourself. I believe that was Wes Rishel.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, this is Wes. Right.

Paul Egerman – eScription – CEO
Yes. I'll ask everyone when they speak. We actually have like two or three different concepts that have just been floated by, so I want to make sure we talk about everything that was just said. The first one from John Houston, if I heard you right, John, you were concerned about duplicate reporting.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Not duplicate reporting, but in the HIO, there's a possibility of having information from multiple sources. If one of those sources does want the reporting to be performed by the HIO on its behalf, you know, pursuant to a business associate relationship, but the other one doesn't, what happens or is there going to be a situation where that HIO again ends up aggregating. Not aggregating data. I shouldn't say it that way. But ends up sending data pursuant to the report that comes potentially from that other provider that has not authorized the HIO to report on its behalf. I apologize if that's not clear, but I'm not sure of a better way to say it.

Paul Egerman – eScription – CEO
Yes. I looked at the data though. I only looked very briefly. It didn't strike me that there was a huge risk because it seemed like it was more identifying either patients or instances. I mean, there was a little bit where they would be asking a little bit of data like test results, but it was mainly they wanted to know what was happening, and so I have a feeling. I don't know how practical a challenge it is, but my suggestion as to how we could respond to your comment, John, is it occurs to me we don't have anybody on the call who works at a public health agency. After we get our recommendation together, let's sort of run it by them, somebody who is an expert in this area, and have them tell us if we miss some issue like the one you're raising.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right, and I think the only area I can think that possibly something like this could occur is if you had two data points from a specific patient that is used to sort of triangulate to determine whether there is some type of disease outbreak, and whether that patient is part of it. One piece of information from one provider may not be sufficient, but when you add it to data from another provider, you might find that that person has some virus or some flu or some whatever that becomes an outbreak and becomes a reportable one. Again, I don't know if that happens or not.

Paul Egerman – eScription – CEO
I was going to make the observation that it's a good question. I would make the observation that in the absence of exchange, there's no way to aggregate that data. And so you're sort of asking about something that sort of becomes available.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'd like to suggest that there's a real simple answer to the question. This is Wes. And that's that the HIO screwed up. It was not authorized to send data to public health on behalf of a provider, and it screwed up. The provider may very well be reporting the data through a separate channel. If we're expecting HIOs to do analytic work by comparing data points, then that's a separate service of the HIO that's different than conveying data to the association. It seems like the HIO has an obligation to know on whose behalf it's sending data where and not to send the data that it's not authorized to send.

Deven McGraw - Center for Democracy & Technology – Director
I think that's right, Wes. This is Deven. John, that sounds to me like a failure of process, and I fear that we can't make policy pronouncements to accommodate where the system potentially breaks down, but I think we've got the infrastructure in place that is the one that needs to be put in place. Then, as Wes mentioned, in that case, the HIO did something that it wasn't supposed to do, and it's arguably actionable at least a breach of contract, if not more.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I suggest then that we make it clear that in the context of an HIO doing some type of submission on behalf of a provider for public health purposes that we make it clear that our recommendation then is that it can only be data provided by or that was originally submitted by that particular provider and not other providers then.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They do have to. This is Dixie Baker.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I'm not sure I understand your point, John, but ….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we're confusing the role of the HIO with the role of the data source. As I understand it, our position is the data source.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The HIO could potentially retain data, and that's the issue. There could be data from multiple providers that the HIO had had.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If there's a lawful obligation for the HIO to report data that its retained rather than under a business associate agreement, then that's a whole different player than we're permitting….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's not my point. If the HIO has data, and let's just assume the provider has the obligation to report. What I'm trying to do is make clear that the HIO, if it is acting on behalf of the provider as a business associate, it is making the report that it can only report data that is from that provider for whom they have ….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I feel like that's in their language now. But it's always a matter of different understandings. Right.

Paul Egerman – eScription – CEO
I agree, Wes. I think what we've got to do is we'll look at the language, but I understand now your point, John. Your point is sort of like no commingling without permission.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's a good way to state it.

Paul Egerman – eScription – CEO
That's your point. Then, Carol, and Wes also had a point. Carol's concern was sort of like a model concern, like if the data is passed through, that's okay, but this should not cause one to retain data. Is that correct?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. What I'm getting at is that we should not imply that the service, if it's being performed for the provider, needs to be opening and using the information that's being passed through. In other words, it is not necessary for the service to retain that information. I do think, by the way, this sort of, and this is a little complicated, but I do think part of the issue that we've just been discussing, and also part of the issue that I'm raising is addressed in the principle of collection limitation and use specification, which is to say, you can only collect the data that you need to accomplish the specific purpose, and you can only use it for that specific purpose. You can't sort, you know, swim more broadly than that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. I think there are a lot of issues that we need to address regarding what the HIO can and cannot do with aggregated data. But I don't think – and I think that those should be on the short-term parking lot.

Deven McGraw - Center for Democracy & Technology – Director
The … lot, not the economy lot.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, but I don't think it's this one because I think that those are really serious issues that need to be separately addressed.

Paul Egerman – eScription – CEO
Getting back to Carol's issue, does the current wording address your issue, Carol? I'm trying to understand how does your issue get addressed.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I don't think it's addressed, and I think we should be explicit about saying in the sentence where it talks about the HIOs performing a service. We should be explicit about saying the HIOs should not or need not pertain that or use that information for any other purpose.

Paul Egerman – eScription – CEO
Yes, except the one comment I would make is, in reading this, we have a wrong way. I assume this service would be primarily provided by an HIO that somehow already was retaining data for other reasons.

Deven McGraw - Center for Democracy & Technology – Director
Yes, well, I'm not sure why you made that assumption, Paul. I think it's – I think we have to, in keeping with our original recommendation, the providers are ultimately responsible for disclosures from their record. But understanding that there is an ability to delegate functions to an HIO as a business associate to perform them on their behalf, I think we need to be careful that in fact our recommendations don't assume an aggregation or collection model or require that such model be put into place.

Paul Egerman – eScription – CEO
Yes. The reason I took….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Can I just say something? I actually was suggesting that we discourage it, and the reason ….

Paul Egerman – eScription – CEO
Discourage what?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
The aggregation or collection of information by a third party in the process of fulfilling a public health reporting requirement. The reason I'm saying that is sort of back to the upstream issue of the best way to protect information from breach or access is not to aggregate and collect it when it's not needed. I am all for supporting the public health requirements, but my worry is in all these population health issues, both for public health quality, research, that every purpose will result in a new aggregation of information and a lot of duplication and redundancy. And I think it's an exposure risk.

Paul Egerman – eScription – CEO
Let me first explain to you, Deven, why I had made that assumption. When I read the materials on this, what I saw was that most of the disclosures to public health agencies, at least in Massachusetts, appear to be all of them or none of them were done electronically. It was all, you have to fill out a particular form, and you have to fax it to somebody. The forms actually were created with this sort of HIPAA principle in mind, so they tried to collect as little data as possible, but that meant that there was a different form for each disease in terms of what you had to collect. It just struck me that if you had an HIO that was on a centralized model, they'd be in a good position to do that kind of – you know, produce that kind of paperwork. To produce that kind of paperwork as a pass through model, I'm not sure how you would do it, if you're going to do that as a pass through model.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
This is Wes. I think we have to recognize that one of the most common, very common function of HIEs today is to do a pass through model of collecting that information, at least for diseases that are identified by a lab test.

Paul Egerman – eScription – CEO
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That is to say, as they pass the result from the lab to the provider by agreement with whoever the obligated provider, I mean, the lab is a provider. The physician is a provider. One or the other or both of them is obligated to report to the public health agency. Just as a byproduct of pass through without retention, the HIO is able to spool that data to public health.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But not all the data. That does require – public – labs are required to report to public health certain types of test results, not all.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Agreed. When it meets the qualifications, then the necessary data can be spooled to public health.

Paul Egerman – eScription – CEO
Your picture then, Wes, it's a different pass through picture than I had thought I had understood what Carol was talking about….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
…the question is….

Paul Egerman – eScription – CEO
…laboratories for other purposes, you happen to notice, well, here's one on a positive test for something, and that goes to public health.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Positive test for sexually transmitted disease, right?

Paul Egerman – eScription – CEO
Yes. You shoot it off to where it belongs.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But I think we're not trying to design the health system here. We're not trying to restrict ourselves to one model or another, except under the kind of consideration that Carol raises where there are privacy implications of one model or another.

Paul Egerman – eScription – CEO
Carol's view, I just want to make sure we get back to what Carol's issue is now understanding the basic…. Carol's view is you want to make sure that this function doesn't create a new opportunity to retain data. Is that what you're saying?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I think we should. Yes. I think we should discourage the collection of that information in any place other than where it needs to be reported. And I would sort of further say, Paul, you know, the whole point of collection limitation and purpose specification, which are based in PHIPS, is to not open the door to, well, let's just collect everything because we might need to report this, that, or the other thing at some point down the road. I mean, that is exactly the kind of slippery slope that I think creates unnecessary exposure.

Paul Egerman – eScription – CEO
I understand your issue, and then it looks like we're having a little bit of trouble getting the wording up on the screen from Deven's e-mail.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I sent it around by e-mail.

Paul Egerman – eScription – CEO
What we'll need to do is we'll just put that down as a note that we need to address that then, that this function should not create additional.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So Dixie has suggested that this is an important enough issue to have an agenda item of its own. I agree with both her and Carol, the problem that I have is with the word "discourage", which is highly nuanced for regulation.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. One other points I think is important to note is a lot of public health authorities have very limited budgets, and they will look at this as an opportunity to be able to have, be able to warehouse, or to get access to data that they simply don't have the systems capability to handle themselves, so I would say that this is going to be an issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
"This" being Carol's point?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, just magnified, I think it's going to happen.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But a public health agency could not ask an HIO to aggregate data.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
That's right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I don't know about that. Public health….

Deven McGraw - Center for Democracy & Technology – Director
I'm not sure they could either under state law.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes. I mean, public health authorities may have very broad rights to be able to seek data and maybe try to make arrangements with HIOs in order to do that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right ….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm always worried about how we balance this issue of controlling the proliferation on any issue, but specifically here, we're talking about controlling the proliferation of replicas of collections of data. I don't want to say aggregates, but collections of data. How we balance that against the general need of various organizations to use business associates to accomplish their lawful function. If a health department makes a business associate contract, well, it's not a covered entity, is it?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Some of them actually act in the capacity of government.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If for whatever reason it makes a contract with a third party to retain information, I don't think we can limit that if that third party happens to be an HIO and the public health department and the HIO are following the principles that Carol set down in terms of collection only for purpose and use only for purpose. Then I don't know how much more we can regulate that. That's why I'm thinking that might be a reason for choosing this middle word "discourage".

Paul Egerman – eScription – CEO
Let's look at a couple of issues. First of all, the public health agencies are set up by state governments, and whatever they do is the result of laws that are passed, and there's a public debate. So these issues where you want to collect PHI on people with tuberculosis, a public debate occurred on that, and so that's all….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
We assume that in the word "lawful".

Paul Egerman – eScription – CEO
That's right.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Variation as well, I mean, if you've seen one, you've seen one.

Paul Egerman – eScription – CEO
That's right. Not only that. They're not necessarily implemented entirely on a state basis. There are local boards of health. There are regional issues, and sometimes with very good reasons because you could have regional outbreaks of issues that people have to deal with. On my screen is the wording. Can everyone see the wording on their screens?

W
Yes.

Paul Egerman – eScription – CEO
So you've got three bullets: the first bullet, public health reporting takes place using the least amount of identifiable data. The second bullet, it says that when the law requires reporting, you can do it. And the third, it says, providers are responsible for disclosure from his or her records, but may delegate lawful, public health reporting to an HIO on his or her behalf. It can do that on a per request basis or a general delegation to respond to all lawful requests. That's the proposal.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Can I make my two points? This is Dixie Baker?

Paul Egerman – eScription – CEO
Sure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Number one, which is straightforward, I think we should add that they account for the disclosure. Number two, I know that this topic has been put on the long-term parking lot, but a lot of public health reporting is done using pseudonymization whereby the covered entity assigns a random number somehow generated that is retained by the covered entity so that the data are sent to the public health agency with a random code, if you will, and only if they need to contact that individual do they go back to the covered entity and

say we need you, covered entity, to relink this, and public health is not allowed to relink that, the covered entity, and now we know business associate of the covered entity is allowed to do that. I think we need to capture two things with respect to that because it is very common practice in public health. Number one is, when they can do pseudonymization versus actual reporting, that's what should be done. And number two, which I think is more sensitive, I'm not comfortable with an HIO being able to relink all of these identifiers.

Paul Egerman – eScription – CEO
Let's go through these issues. First, on accounting for disclosure, I mean, while I agree with you 100%, I think we're going to handle accounting for disclosures as a separate topic. Is that what …?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. Public health gets a special – it's handled special in HIPAA. Just like for meaningful use, we've captured meaningful use here. Not meaningful use. Just like minimum necessary we've captured here, we also need to capture accounting for disclosure because public health is sort of an exceptional case. It just says public health means that you give it to them. I think we need to explicitly say that it needs to be the minimum necessary, and the disclosures need to be accounted for.

Paul Egerman – eScription – CEO
Somebody typed on the first paragraph at the end, "Providers should account for disclosures". Does that respond to what you're saying, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Thank you.

Paul Egerman – eScription – CEO
And the second paragraph, I can't pronounce that.

Deven McGraw - Center for Democracy & Technology – Director
I think pseudonymization is a form of using less identifiable data, but I don't know that we want to anoint it as the way….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
…standard….

Deven McGraw - Center for Democracy & Technology – Director
…perfectly acceptable and may be even recommended practice for a way to send public health reports in least identifiable fashion, but preserving the ability to link them up at the covered entity level when that needs to happen.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If you look at the HITSP standard, pseudonymization, there's a whole standard on how to do it, and it's so much a part of public health that it's actually part of the HITSP use case for public health that's commonly done.

Paul Egerman – eScription – CEO
But let me raise a different issue. Why should we be telling the public health agencies what they should be doing? Isn't it up to them to …?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

We're telling the providers what they should be doing, and respond to a request from public health, but I'm questioning, if the HIPAA law and subsequent regulations are saying one thing, are we going to say another thing in a policy recommendation? If so, what does that mean? Are we recommending new regulations or what are we doing? If it's just not clear, then I think we should try to clarify.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
This is Adam … something.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Adam, go ahead.

Paul Egerman – eScription – CEO
Adam, please, yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Under the current accounting standard, which has been around since 2003, public health disclosures are accounted for. All HIPAA covered entity providers are currently required to account for all disclosures for public health, so whether you want to kind of reissue that as part of these recommendations, I leave that up to you, but I just want to provide that as a background….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What about minimum necessary, Adam? Does it also require minimum necessary?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Hold on. If anybody has looked at a public health request for information or these types of things, they're very prescriptive typically in what they expect you to send.

Deven McGraw - Center for Democracy & Technology – Director
That's covered under these recommendations.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Although let me clarify on minimum necessary. This is Adam again. HIPAA does require the covered entity be disclosed to minimum necessary information for public health, but there is a provision that says the covered entity can rely on the public official statement as to what is the minimum necessary, which is something that I would suggest you discuss here is who is in the best situation to decide what is the minimum necessary for purposes of public health. Is it the provider of the HIO, or do they have to potentially rely on the public health…?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The public health authorities typically will tell you what they want, and I don't think you have much. You typically don't. Especially if it's mandatory reporting, you don't have a lot of discretion of what you send.

Paul Egerman – eScription – CEO
That's right.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right, but that is not true for the HIO. The HIO, in fulfilling this function, can presumably collect what it wants in order to report what is required by public health.

Paul Egerman – eScription – CEO
Right. We've got more than one issue here on the table, and so you're raising an interesting issue, Carol, but let me make sure. Right now, I think we're running a little bit with some of the Dixie's issues. Dixie wanted to talk about providers should account for disclosure. Adam said, well, that's already in the law that we have to account for this. Do we need to put that sentence in?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, this is Dixie again. I think, if the accounting is already there, and minimum necessary is already there, then we should not include either one. But I think, including one and not the other sort of creates some….

Paul Egerman – eScription – CEO
We can include them both. It's not a big deal. The other one is this controversy about pseudonymization.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Pseudonymization.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I want to make clear that I'm not enamored with the word itself. All I'm saying, I think that they should be, you know, the ideal would be de-identified data. But if that's not possible, I don't think the second should be PHI. The second should be, can I report it using with a coded identifier instead of the real identifier, and then the cord of last resort should be PHI. That's all I'm saying.

Paul Egerman – eScription – CEO
Deven, you didn't think we needed to do this.

Deven McGraw - Center for Democracy & Technology – Director
I certainly don't mind mentioning it, but it's an example technique or a best practice. I don't know that we should be in the position of saying though shalt use X necessarily. I disagree with….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
There's middle ground there.

Deven McGraw - Center for Democracy & Technology – Director
…use the least identifiable data possible where the law provides the provider with some discretion about what to send, which often is not the case. But when it is, they need to use it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
There may be a possibility of words that imply it's not a polar choice, that there are more than, I mean, the least possible implies that in some sense, but I think the rest of the wording tends to imply it's either identified or it's not identified.

Paul Egerman – eScription – CEO
They're typing something into the system like techniques, including pseudonymization should be considered as approaches. Perhaps that responds to your issue, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Like I say, if Deven would prefer that be a coding of the identity of the individual, use that instead of the word, that's fine with me too.

Deven McGraw - Center for Democracy & Technology – Director
I'm fine with the word. I don't have a problem with the world.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then my only problem is it's misspelled.

Deven McGraw - Center for Democracy & Technology – Director
Yes. There's a "y" in there. We'll take care of it later, Dixie.

Paul Egerman – eScription – CEO
We'll fix that later. That's a variation of wordsmithing is word spelling, and so we will get that and identifiable respelled correctly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would defer to Wes because what he said is what I think should be said that it's not either/or. It's a continuum of alternatives.

Paul Egerman – eScription – CEO
Now I want to make sure we capture Carol's concern also, which is, if I understand it right, Carol is saying in this process of an HIO transmitting information, somehow the HIO cannot unnecessarily retain or collect data. I'm wondering if there's a way that you can just – something that's being typed right now, but if you can suggest wording to capture your thoughts, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Well, I have a question, I guess. The three principles that we've been discussing, the high level principles, which I think will apply to all of the issues we're going to discuss today, both quality and public health, are they going to be articulated anywhere? If they are, I think it makes it a little simpler, and the fix here is smaller.

Paul Egerman – eScription – CEO
When you say the three principles, what are the three principles you're referring to?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Collections, limitations, use limitations, and what am I missing? And specification.

Deven McGraw - Center for Democracy & Technology – Director
Purpose.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
What was the third thing?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Purpose specification. In other words, you have to specify the purpose for which you're collecting information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's not the same as collection limitation?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No. You can specify the purpose, and then collect more.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I see. Okay.

Paul Egerman – eScription – CEO
You're suggesting that we….

Deven McGraw - Center for Democracy & Technology – Director
They're inextricably linked.

Paul Egerman – eScription – CEO
You're suggesting we clearly articulate those three principles as like a foundation kind of document or foundation for all of these questions?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm saying there are overarching issues for all of the things that fall in population health, not necessarily specific to public health, and that if we do that, we don't have to keep repeating some of these, and you can't use it for any other purpose, and you should only collect minimally what's necessary. Do you know what I mean? In other words, it's a way to make the recommendations that are specific to public health and quality a little bit more parsimonious.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I agree. I tried to describe it as meta-policy in an e-mail last night under the anything you can do, I can do, meta rule.

Paul Egerman – eScription – CEO
Can you, Carol, suggest wording for these three principles for us?

Deven McGraw - Center for Democracy & Technology – Director
This is Deven. It has the advantage of being that sort of collection of fair information practice principles was already adopted by the policy committee. In many respects, we are reminding them and applying it specifically to population health uses.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I'm finally on the call, and I've been listening for the last few minutes, and I want to say I'm totally in accordance with the direction you're going, but I wanted to also add about the retention of the data. I think we need to really have a discussion on how long this data is retained and what happens to it while it is in possession of public health entities.

Paul Egerman – eScription – CEO
Excellent comments, Gayle. Welcome. We actually are going to get to retention data in one of the subsequent questions. What I'd like to do is see if we can wrap up this question because this is still question number four. We have five more to go. Is what's on your screen a reasonable response to question number four? Does anybody object to saying this works and able to go onto question number five?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I don't think we've completely addressed these issues unless there's another place to address it because I still think the implication here and, Paul, your interpretation of it earlier was a good one. I still think the implication here is that if the HIO is performing the service on the provider's behalf, the implied message here is that the HIO should aggregate that information and collect it and retain it. If we're going to get to that issue as a meta issue….

Paul Egerman – eScription – CEO
That's right, and we inserted this sentence. I don't know if it's worded right, but … may not unnecessarily retain data. We really have to expand out.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Unnecessarily, you know, just because you want something doesn't mean you need it. I don't know that unnecessarily is – I don't know that the HIO may not unnecessarily retain data. For me, it's not necessarily the right way to say this.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I think the common use case for HIOs is there will in fact be a lot of data retained for the purposes of care coordination and other services in the community. It may be that if nothing – if they existed for no purpose other than public health reporting, these recommendations would make sense. But that's the tail wagging the dog.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
But we're talking specifically about public health, and they may be collecting information that is sensitive to fulfill a public health purpose that has much less to do with care coordination or any of the other issues, and is not specifically collected for any of those other issues. I do think that we want to make sure, especially for sensitive data, that we don't redouble the risk of exposure by encouraging lots of replicated databases with that information.

Paul Egerman – eScription – CEO
What do you propose that we do, Carol?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
My proposal earlier was that something along the lines of when the HIO is acting on behalf of the provider, they should, and maybe it goes in the first sentence. They should not be or they should be discouraged from retaining information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I seriously think we should consider taking Carol's principles and moving them to the head of all of these questions and addressing variances to the principles only when variances exist because I think we're going to have this same discussion over and over again.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

Gayle Harrell – Florida – Former State Legislator
I think you're right. This is Gayle.

Deven McGraw - Center for Democracy & Technology – Director

This is Deven. Move the sentence—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we can leave the sentence out, if in fact all of these questions are headed by a general statement that represent the three principles that Carol has outlined.

Deven McGraw - Center for Democracy & Technology – Director
Right. Moving that up to the front should apply to providers or an HIE use of access, use, or disclosure of data for this function.

Paul Egerman – eScription – CEO
If I'm hearing your comment right, Wes, and Carol's comment right, if we have our principles laid out correctly, our answer to this question is simple.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

Paul Egerman – eScription – CEO
It's as simple as, yes, providers can ask an HIO to do this for them, either on a sort of universal for every case or on a specific, per request basis, based on the other principles.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right, and without our having to add anything, we'd be implying that such an agreement constitutes authorization to deal with certain data, however they deal with it. They might retain it. They might pass it through, but if it's for a specific purpose, used only for that purpose, and that does imply that in the general case that David described where they are using data for continuity of care, the same data will be collected for multiple purposes, and the retention and use will be specific to the purposes.

Paul Egerman – eScription – CEO
Right. Basically we have a response to this question is like a two-sentence response, which is the principles of collection limitation and use apply and, under those principles, a provider may delegate their responsibility for public health reporting to an HIO on a per request basis or on a auto disclosure basis. And so that's our answer to question four. In terms of wordsmithing these collection limitations purposes, paragraphs, we'd probably have stuff that's pretty close here on the screen, but let me suggest that we do that as sort of like one of these offline processes. We'll sit around the wording and make sure everybody is comfortable with it.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
That's good.

Paul Egerman – eScription – CEO
Does that work for everybody?

Gayle Harrell – Florida – Former State Legislator
Paul, may I bring up one other issue? We're talking about – this is Gayle. We're talking about the provider giving that responsibility or allowing the HIO to send that information for them either on a per individual basis or broadly across the board. What is the ability of the health department to query and go to the HIO and query and say, I want to know everybody who has gonorrhea? This is mandatory reporting. Does that empower the Department of Health to do that?

Paul Egerman – eScription – CEO
I don't think what we say empowers the Department of Health to do that. There may be other issues that you're raising, but nothing we're saying empowers the Department of Health to do that. It's an interesting question that you're raising. You're sort of saying, well, does the Department of Health have free rein to run all over what is going on at these HIOs, and I don't think they do.

Gayle Harrell – Florida – Former State Legislator
We're looking at things from the provider perspective in reporting, but there's a converse of that. If there's mandatory reporting, does that not open the door, and are we empowering then to have the query go the other way?

Paul Egerman – eScription – CEO
I don't think we've done anything that empowers the public health agency to take any action, and so the only way that that could happen, what you're describing, Gayle, would be if a state legislature passed a law that permitted it.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
If there was a public debate, and the legislature passed a law that permitted it, then it would be permitted. But another way to look at it is you look at our second recommendation that we made at the last policy committee meeting. We talked about how you would authorize providers. When we get through this whole process, there should be a clear description of who is really authorized to access this information, and public health agents, you know, employees of public health agencies weren't the definition of a provider who had access to this information.

Gayle Harrell – Florida – Former State Legislator
I think that is the conversation that perhaps needs a little more legal clarification because it is, if that is mandatory reporting, why would the health department not have that ability?

Deven McGraw - Center for Democracy & Technology – Director
They do, but we haven't given it to them.

Paul Egerman – eScription – CEO
Yes. To the extent they have it, Gayle, it's not coming from us.

Deven McGraw - Center for Democracy & Technology – Director
If they have it, then entities have to comply.

Paul Egerman – eScription – CEO
Yes. If the state law says they have it, then they have it, and my guess is, in many states, if they don't have it, they'll get it. And the reason why is a lot of these HIOs will be run directly or indirectly through the Department of HHS, and that's running the public health agency, and they're going to put one and one together.

Gayle Harrell – Florida – Former State Legislator
Yes. Okay. I just wanted to make sure that this was not something that we were empowering. We are strictly looking at this from the reporting element of the provider through the HIO to the Department of Health.

Paul Egerman – eScription – CEO
That's correct. That was what the question was that we were answering.

Gayle Harrell – Florida – Former State Legislator
Yes.

Paul Egerman – eScription – CEO
We've answered question number four. Let's move on to question number five.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Sorry. Can I just raise one more issue on four, and this is probably … to the retention issue, but is it possible we could say, in the identifiable section, something like more identifiable data should be subject to higher levels of protection?

Paul Egerman – eScription – CEO
It's a good question, but I'm not sure it's relevant specifically to question number four. That might be relevant to the wording of the basic principles that we put forward.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I agree.

Paul Egerman – eScription – CEO
We're going to talk about sensitive data separately, and so that that also could be a place where some of your concerns might be addressed because a lot of the public health reporting does deal with sensitive data because it deals a lot with sexually transmitted diseases, and so there could be some issues there. I would like to move on to question number five, which is on slide 14, which is a similar question, which is how should quality reporting be handled. The issue here, when you get to slide 14 on quality reporting, it's sort of like we're doing the three-legged stool. The three-legged stool is, we've got treatment coordination. We've got public health, and we've got quality reporting. Those are the three areas that sort of the meaningful use that the tiger team is trying to address this summer. My question on this is, does our answer for public health apply to quality reporting? What's different about quality reporting that means that we would answer this question differently?

Deven McGraw - Center for Democracy & Technology – Director
The other parameter—this is Deven—that I want to make sure we keep in mind is that we set from the beginning that we were talking about the quality reporting required under meaningful use. So it's reporting to CMS. It's not all quality reporting. And it's already stated to be summary data.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
You're right. It's already. That's what I was going to say. It is already stated to be summary statistics, not identifiable data. So it fulfills in some ways the principles that we have. The slippery slope for me, and this is language I recommend we take out of both is in accordance with HIO's policies because they may be different than what CMS is requiring, and I think we don't want to go here.

Paul Egerman – eScription – CEO
Yes. In accordance with HIO's policies was an alternative. It was not a recommendation.

Deven McGraw - Center for Democracy & Technology – Director
Yes. In the revised recommendations that we had on the screen earlier, I don't think it was in there at all.

Paul Egerman – eScription – CEO
Is the answer to this one simple? As authorized by the record holder, the record holder may authorize electronic auto disclosure?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I guess I'm, you know, you miss one call, and life passes you by, but why are we limiting quality reporting, the help of an HIO and quality reporting to what is required by, in order to qualify for an incentive, as opposed to quality reporting in order to get paid? What is there about that that makes a difference in the way we're addressing as policy?

Deven McGraw - Center for Democracy & Technology – Director
Wes, it's Deven. It was just an attempt to keep the discussion more focused so that we were able to make some decisions, and we could, of course, parking lot, in daily or economy, the issues that would still need to be resolved that were sort of outside the realm of stage one of meaningful use, but were likely uses of exchange either at an early or….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So we're going to put this one in the lot where you find your car on bricks and the tires gone.

Deven McGraw - Center for Democracy & Technology – Director
Right. We don't even have payments on the early list. It was really an attempt to be more focused.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's Fine. Okay. Thanks.

Paul Egerman – eScription – CEO
The way to respond to your concern, Wes, is remove the word "required".

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
There's no need to respond to my concern. I'll be okay.

Paul Egerman – eScription – CEO
On the quality reporting question, assuming that we have these basic principles worked out, is this a reasonable response, as authorized by the record holder?

Rachel Block – New York eHealth Collaborative – Executive Director
This is Rachel. I'm sorry. I'm kind of with Wes here. The way that we're making it clearer that we are limiting this to that particular scenario is how? Is it in the considerations?

Deven McGraw - Center for Democracy & Technology – Director
It was in the early part of the slide, so we would have to have that be part of our presentation to the policy committee that this was the sort of universe of exchange that we were focused on for this set of policies.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I kind of like Wes' concern as well because I think there are a number of HIEs that are considering quality reporting as a means of sustainability, and they would not limit it to meaningful use, but to the many different kinds of quality reporting, as required, including private insurers, perhaps. So it's going to come up pretty quickly for the HIEs out there in the real world, broader than just meaningful use. Maybe we don't need to comment on it, but it might be useful if we did.

Paul Egerman – eScription – CEO
If you take out the word "required" I think you've solved that. It just strikes me also, this is an HIO performing a valuable function, especially for small hospitals, small physician groups to handle it. The HIOs are looking for a business model, and this is a valuable function that they could perform that would help everybody.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If we can get closure on it, then I think it would be an improvement, and your suggestion is helpful, I think, Paul.

Carl Dvorak – Epic Systems – EVP
Paul, this is Carl. I wonder if we could say, as authorized by the record holder under a business associates agreement.

Gayle Harrell – Florida – Former State Legislator
Very much so.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I think, in many respects, some of the principles that we laid out for the public health reporting are worth repeating, including the HIO performs functions on the behalf and at the direction of the provider who has the primary responsibility for disclosures from his or her record, and that happens through a BA agreement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with Deven. I would just copy what we said about public health and replace quality with it. Every single thing we said there is applicable here.

Carl Dvorak – Epic Systems – EVP
The only difference—this is Carl again—is that for public health, you've got the background law that creates a set of definitions you operate by. Under quality reporting, if you want to make it just CMS, then I think we're okay with the narrow definition. But if we want to open it up to all quality reporting, I think it needs the background of a BA agreement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
In either case, I think we need a BA agreement.

Deven McGraw - Center for Democracy & Technology – Director
We need a BA agreement with the HIO, even to the CMS….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know that in some cases things are, activities are being performed under the banner of quality monitoring, and I think that we do need the constraints that we put, we need to put the constraints into place exactly like we did for public health, the minimum necessary, etc.

Gayle Harrell – Florida – Former State Legislator

I think you could just repeat what was in the public health recommendation and the principles that establish that….

Paul Egerman – eScription – CEO
Good comment, Gayle, because what is being written here is close. If you look at the second paragraph, we really should probably lead with it. The principles of collection limitation purposes should apply. This is just repeating the same principles that we're going to apply to the public health thing, and then we have this other sentence. It doesn't matter what order they're in. As authorized by the record holder under a business associate agreement, the record holder may authorize electronic … disclosure pursuant to quality reporting. Do you want to add "to CMS"? Is that what you're …?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think that is what we're…. I think we're talking broader.

Paul Egerman – eScription – CEO
Okay, so then we don't need the "to CMS", so do these two sentences capture what we want to do?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Hang on. I've got to open up my screen. I'm getting blind.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I think it comes down to the value that we felt that the specific bullets in the previous one added.

Paul Egerman – eScription – CEO
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If they significantly added to value to the public health one, I would think they would significantly add value to this one as well.

Paul Egerman – eScription – CEO
By putting in that sentence, we're sort of like inheriting all of those principles to this recommendation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I don't … rules of inheritance in place here.

Paul Egerman – eScription – CEO
Pardon me?

Deven McGraw - Center for Democracy & Technology – Director
I think probably the way we're going to need to formulate this, Paul, is to maybe condense these recommendations so that we can use some of the same principles for both.

Paul Egerman – eScription – CEO
Yes. I agree. We'll do that, and does this work for everybody then? We're going to have the principles

for both, and we're going to have the sentences authorized by the REC holder under a DEA agreement … a record holder may authorize electronic … disclosure pursuant to quality reporting.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm okay, subject to our review, I guess.

Deven McGraw - Center for Democracy & Technology – Director
Yes. We'll take a look at them.

Paul Egerman – eScription – CEO
Again, we're going to look at everything when we get all done. Again, we can wordsmith it separately, so if we're okay with this, it's a great success. Let's move on to the next slide, which is slide 15. Deven is going to take us through this one.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Actually, I think that some of these issues have begun to come up in some of our earlier conversations, and maybe this is the place to land on some of the more specific recommendations. This slide deals with what limits, if any, should apply to third party service providers regarding data reuse, and I would include HIOs and any business associate, intermediary, as a third party service provider. This was an attempt to try to define it in a way that captured the entities that provide functions in the middle, including an HIO. Then there's a subsequent set of two questions about – so you have this first one is about limits on reuse. The next slide is about retention periods. Then the third slide is about transparency about third party service providers. This is the sort of bucket of questions related to limitations on parties in the middle. Then we have a subsequent question regarding whether the BA agreement is adequate as an enforcement vehicle for those limitations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I have a couple things to say about this one. Obviously this is a very important one.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
My initial reaction before I read the NPRM actually was that I agreed with essentially number one, except that I would say, I would drop everything after the parentheses, and I would change reuse to use so that it would read, "may not use for any other purpose, except as reasonably necessary to fulfill third party service provider business functions, as specified in the agreement". That opinion was reinforced by the NPRM. The NPRM has some really nice clauses in it about how a business associate can only do those activities that are explicitly specified in the business associate agreement.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And, you know, you could almost, I have a couple that I picked up out of there. You could almost just lift them, you know … a business associate may use or disclose protected health information only as

permitted or required by its business associate contract. Those kinds of things, I think, are what needs to be captured here, and the term reuse should be use.

Deven McGraw - Center for Democracy & Technology – Director
That's a fair point, Dixie.

Paul Egerman – eScription – CEO
This is Paul. I responded to this issue from the standpoint of somebody who I used to b a CEO of an organization that was a business associate, so I used to have to sign a lot of these business associate agreements. And on the one hand, I completely agree with what you just said about, may not use for any other purpose. The problem with it, I always have from my perspective is, well, perhaps that wording is so broad that it's hard to know what the purposes are. I was always more comfortable with the situation where I would be able to disclose what I actually do with the data. In other words, here's how I retain it.

Look at the issue of retention for example. How do you decide what the right retention time period is? There's no right answer to that question. To me, the best answer was to simply say, well, this is what I do, and if you want to know why, I can explain why. But I just always thought that was – I don't know how to describe it. It was a more practical way of doing the exact same thing because if you're disclosing something, and somebody says, no, you can't retain the data for 100 years, and you can't retain the data for 5 minutes. Neither one of those work. And so they'll tell you if you're doing it wrong, and so maybe there's a way to take option one and merge with option two. But I think what's discussed in option two where you disclose your record retention policies and procedures is, in a practical way, more valuable than what it says in option one.

Deven McGraw - Center for Democracy & Technology – Director
Paul, this is Deven. My concern with what's in, and don't delete that yet, please. My concern with what's in option number two is that at least the initial clause sort of treats the BA as though once it gets the data from a covered entity, it has some freedom with respect to how it acts, you know, uses or discloses that information in the future, as long as they're doing so in accordance with applicable law, rather than consistent with the concept that a BA gets data from a covered entity in order to perform a specific function or a set of functions, and that is how they got the data in the first place, and that ought to come with a set of limitations that don't give you the full rights necessarily that a covered entity had unless, of course, the covered entity in fact gives you specific rights.

But my concern was that at least may retain, use, and disclose in accordance with applicable law felt a little too broad to me, but I totally get your point about the retention piece. And so it almost feels like this recommendation may ought – that a reasonable recommendation in this area may start with, as we did with public health reporting and quality reporting, you know, the sort of principles of purpose specification and collection and use limitations. With respect to data retention, I think you're right that there's no one size fits all. That in fact entities need to have policies about how long they need to retain data, but that data retention has to be consistent with the purposes for which they collected it and the limits on the use that are in the business associate agreement.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I have a major problem with number two because I think that is way too broad, and if there's going to be anything that happens with that data, it needs to be the holder, the owner of that data or owner, whatever, the provider of that data needs to know exactly what's happening, and also needs to control that. Anything applicable under law is a very broad category, and I have a major issue with that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. I think, number one, as I suggested we revised a while ago is, right, except that we have to add the disclosure and retention because it doesn't capture those two in it. But I agree with Gayle. Saying we have to obey the law says nothing, and it's our responsibility here to recommend policy, and I think that the policy should be that a business associate retains and uses or discloses and uses information and retains only as specified in the business associate agreement, consistent with our principles.

Gayle Harrell – Florida – Former State Legislator
Absolutely, Dixie.

Paul Egerman – eScription – CEO
Yes. What I'm trying to say is we have to specify something more than just say we're going to do what is reasonably necessary because that also is broad. That's a restatement of the law.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Where's reasonably necessary? Up here in the….

Paul Egerman – eScription – CEO
Yes. May not use for any other purpose unless as reasonably necessary to fulfill the business function. Well, I have to say, I'm thinking about what Gayle said, and that's also broad.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Let me explain to you why….

Paul Egerman – eScription – CEO
To me, you have some combination where you say that, but you also say what you really do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
No, absolutely. This is Deven. Just so that you understand why I put that in there, you sort of have a set of functions that a business associate is specifically asked to perform, and then there are likely some business operations that are related, directly relate to the performance of that function that the third party would need to be able to use the data in order to perform. It was just trying to find a way to capture – not to expand uses of data beyond the parameters of the business associate agreement, but to acknowledge that a BA and performing a set of functions probably has some administrative tasks.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's exactly the word that the NPRM uses is administrative tasks associates with fulfillment of the terms of the BA.

Deven McGraw - Center for Democracy & Technology – Director
Yes. It's a much better phrase. Thank you, OCR.

Paul Egerman – eScription – CEO
Basically what I'm saying is all of the kind of wording we have in section number one is fine, but….

Deven McGraw - Center for Democracy & Technology – Director
Paul, I'm not sure why, but there's this piercing noise when you talk. Is it just me who is hearing it?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No, I heard it too.

Gayle Harrell – Florida – Former State Legislator
No.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
It sounds like Morse code.

W
Unfortunately, Paul, we're tracking it as coming off of your line.

Paul Egerman – eScription – CEO
Do you want me to call back on a different line?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. That would be helpful.

W
Would you be able to?

Paul Egerman – eScription – CEO
Sure.

W
Thank you.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Now what are we going to say while he's gone?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Talk about Paul.

Deven McGraw - Center for Democracy & Technology – Director
It sounds like where we're landing here is, again, consistent with the fair information practices of purpose, specification, collection, and use limitations that in fact, there are limits on what third party service providers could do, and that is, it's limited by what the covered entity has allowed them to do pursuant to the business associate agreement and administrative tasks that are consistent with those core functions.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Deven, I have a question, which is that we go out of our way to say record holder here, but are we saying that the record holder, which I'm assuming is the provider, is always in the position of basically making the determination of what purposes are permissible? In other words, the record holder may agree, but the patient may not. I mean, there are some purposes where, I don't know. To me, it sounds like we're saying that the provider can agree on behalf of the patient to whatever purpose it is, and….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I second Carol's concern, and I think it actually cuts on the other side as well. If, for example, the BA that the covered entity is sending data to is the patient's PHR, it's not the covered

entity's role to determine what the patient does or doesn't do with that data once they've received it. It's not so simple to simply say that the covered entity can restrict what the business associate does, although I totally agree with the spirit of that.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I had conceived of the question as being limited to third party service providers contracted to provider record holders versus in the context of a PHR, the relationship is between the patient and the PHR. Of course, any downloaded data is done with individual authorization. And a provider certainly can't delegate a function to a BA without the patient's authorization is patient authorization is required. What exactly do we want to articulate here?

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I think we need to put some specific statement in as to the patients' rights so that, first of all, for transparency that the patient had some knowledge that there's a third party entity dealing with the data, and also that this is for treatment, payment, the normal things for which a provider has the ability to do things without direct authorization.

Deven McGraw - Center for Democracy & Technology – Director
Yes. We can either expressly acknowledge that none of the above statements is meant to bridge or undercut the right of patients to authorize access, use, and disclosure of their information.

Gayle Harrell – Florida – Former State Legislator
Exactly.

Deven McGraw - Center for Democracy & Technology – Director
And is really talking about third party service providers who are contracted to provider record holders and not PHR vendors where it's an independent PHR being offered directly to the individual.

Gayle Harrell – Florida – Former State Legislator
I thought we had parking lot the PHRs anyway.

Deven McGraw - Center for Democracy & Technology – Director
We are parking lot PHRs, but I think that I just want to make sure that people don't misread the question since it's fairly broad as potentially applying to a PHR vendor, which some might argue is a third party service provider.

Gayle Harrell – Florida – Former State Legislator
Have we talked about transparency here because I think that's…?

Deven McGraw - Center for Democracy & Technology – Director
No, not yet. We have a transparency question. Can you just hold it for…?

Gayle Harrell – Florida – Former State Legislator
….

Deven McGraw - Center for Democracy & Technology – Director
And it's not even in a really far parking lot, Gayle. It's due to come up on this call. I just want to make sure we have the right set of – we have some draft recommendations to massage on the sort of limitations on use and reuse and retention periods.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, I don't think what we have on the screen in that second paragraph reflects what we agreed upon at all.

Deven McGraw - Center for Democracy & Technology – Director
I'm sorry. I haven't had a chance to read it. I've not been looking.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What we agreed upon, it said may not use, disclose, or retain for any purposes other than those specified in the business associate agreement and administrative functions related – related administrative functions.

Deven McGraw - Center for Democracy & Technology – Director
Right. In other words, the use and disclosure of information by a third party service provider is limited to those functions for which that are covered by the business associate agreement and administrative processes that are directly related to those functions. My only question is about whether you are telling – whether you're saying that covered entities can specify a retention period for a business associate. Maybe they could, but I'm just thinking about whether….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes … actually meant by retain here … says to retain, not retention period, right?

Deven McGraw - Center for Democracy & Technology – Director
Right. They shouldn't retain it for any longer than is necessary to perform their function.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, but all the rest of this from that cursor on is this other stuff or as specified. We need to delete. It may not retain, use, or disclose for any purpose other than those specified in the business associate agreement.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Do you have that, Linda?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Actually, for completeness, my apologies, it can't be just a business associate agreement because often it will be an agreement with a provider, I'm sorry, with a business associate to perform a function. Then you slat to it a business associate agreement, so there is typically a written agreement as to some service being provided, as well as business associate terms that are included. So you need to be more specific and say that it is also related to a function that is permissible, an agreement for a function that is permissible for a business associate to perform on behalf of a provider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It still has to be in the agreement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But you said specifically a business associate agreement, and I just want to make sure that people don't misunderstand that as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Those words are what are in the NPRM.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm just telling you that….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
…require the business associate….

Deven McGraw - Center for Democracy & Technology – Director
Right. John, say specifically what you would want to see.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It would be to fulfill the service provider's responsibility within a written agreement with the provider and consistent with its obligations under a business associate agreement, something like that.

Deven McGraw - Center for Democracy & Technology – Director
I'm not sure I understand the distinction.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Deven, this is Adam.

Deven McGraw - Center for Democracy & Technology – Director
Adam, go ahead.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
This is somewhat addressed I our sample business associate provision that … back in 2003 where, for example, there's generally going to be a service agreement, and the business associate provisions may be on top of that, and we list it as options. For example, you can specifically list the uses and disclosures that the business associate may do. Alternatively, you can point back to the service agreement and say, you may use and disclose pursuant to kind of the service agreement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Let me just say this. Almost all providers use a pro forma business associate agreement, something that they simple – and I'll typically reference it within a service agreement. I'll reference the terms inside a service agreement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Ours are backwards for that. Ours are a business associate agreement, and the attachment is the specifics that you're referring to.

Deven McGraw - Center for Democracy & Technology – Director
I don't want to get tied up in….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I want whoever is driving to delete the rest of that paragraph. There are all sorts of things we don't want there.

Deven McGraw - Center for Democracy & Technology – Director

I know. I think she's catching up with us, Dixie. I think we're doing form – I think some of this discussion is a little bit of form over substance. I want to make sure we're agreed upon the substance.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But this is substantive though, Deven, and I'll tell you why. Because people will look at this and say that the business associate agreement are these pro forma contracts that often are very generic, and there is a separate service agreement that typically has much more detail and more specifically describes the services being performed. That's all I'm trying to do is make sure it's clear.

Paul Egerman – eScription – CEO
Yes. This is Paul. I'm back. You'd respond to that … specified in the BA agreement. You could say the BA agreement, parentheses, including service agreement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That would be more … yes.

Deven McGraw - Center for Democracy & Technology – Director
That's fine.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
How about…?

Paul Egerman – eScription – CEO
Or … service agreement.

Deven McGraw - Center for Democracy & Technology – Director
I just lost the screen, so I have no idea….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Or say, and related to service agreement. I think that's right, Paul.

Paul Egerman – eScription – CEO
Yes, and related to service agreement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Why don't we make it exactly what's in the NPRM, and then at least we'd be parallel?

Deven McGraw - Center for Democracy & Technology – Director
Yes. No, I think we can do that. We'll make sure that we are not overly reliant on using the term BA agreement, and make sure we either say BA and service agreement. John, my point was that the substantive point is that a third party service provider use of data is limited to what's permitted by that service/BA agreement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right. I agree with that.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Deven, this is Adam. What about required by law situation? For example, the health information exchange receives a court order.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Good point. We're not trying to trump law here. Yes, I mean, I think we'll go back into the NPRM and pick up some of that good language. Dixie, if you want to send or draw our attention to those phrases that caught your eye, I'm sure I underlined them too, but you'll just save me time.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure. I'll do that.

Paul Egerman – eScription – CEO
Adam, the required by law is almost always included in the BA or the service agreements too. Everybody acknowledges they've got to do it. You got a subpoena, you do whatever it says to do.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
So nobody complains about that one.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think you have an option.

Paul Egerman – eScription – CEO
That's right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think the only case for us is do we want to acknowledge that option, or do we risk someone commenting, inferring that we've ignored that option?

Paul Egerman – eScription – CEO
While we were talking, they put in an "or as required by law".

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
All right.

Deven McGraw - Center for Democracy & Technology – Director
… so we don't get a question about it, and I think that's a good point, Wes. We might forego a question from a policy committee member if we expressly state it upfront. Now we have here at the very end of this policy recommendation, require disclosure of record retention policies and procedures.

Paul Egerman – eScription – CEO
That really leads to the next question.

Deven McGraw - Center for Democracy & Technology – Director
Yes, which is closely related to the question on the next slide, if we can go to the next slide, which is regarding what limits, if any, should be applied to retention periods. I'm waiting for us to … here we go. I put up a straw proposal here. I'm not sure if I still love this wording, but it essentially says that the third party service provider/business associate may retain data only for as long as reasonably necessary to perform the functions requested by the data holder. I said in activities reasonably related to these functions, but maybe we can use that administrative functions reasonably related. They have to establish retention policies, and at the end of the data retention period, they have to either return the data to the

covered entity securely or destroy it per those NIST standards. This was the straw proposal that we came up with for your consideration.

Paul Egerman – eScription – CEO
Yes. Deven, this is Paul. My response, I probably should have made that response on this question as opposed to the previous one. The comment I made before is I think that that's good, but you have to add the concept that you're going to require a disclosure because it's just reasonably necessary for data retention is actually broad. It's much better to just say what the plan is.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
You have all of that, but you have to add, and required disclosure of the retention policies and procedures.

Deven McGraw - Center for Democracy & Technology – Director
Right. Yes, I think that makes sense.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Add that to number, for the first line.

Deven McGraw - Center for Democracy & Technology – Director
Yes. So in other words, it is recommendation one. It's the parenthetical regarding the ability to retain data also applies to administrative functions that are reasonably related, and retention policies must be established and disclosed, and then the rest of it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. I'd also like to see us add minimum necessary and encryption at rest.

Paul Egerman – eScription – CEO
Encryption at rest is like a whole broad issue that's not, it's like a totally different topic.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's a rat hole.

Paul Egerman – eScription – CEO
Yes. I mean, I had a conversation with the CEO of a large health information, HIT company, and he was just, you know … he was unhappy about encryption at rest.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is not a provider organization. This is an HIO with a lot of data from a lot of different organizations.

Deven McGraw - Center for Democracy & Technology – Director
Depending on their model. They don't necessary. We don't need to suggest that HIOs are only models that collect data.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, we aren't, but if they do, if they do, I think that they need to protect it at a higher level than a provider should be required to protect.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
You still need to be considerate of the financial impact because encryption at rest from a CPU capacity, as well as an encryption perspective could cost millions of dollars to implement, and that's then reflected back to the providers potentially, so there are other considerations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's too bad. It's all based on risk management.

Paul Egerman – eScription – CEO
Yes, but I….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I….

Paul Egerman – eScription – CEO
First, Dixie, I think you raise an excellent issue, which I'm very familiar with. I'm going to give you a legalese kind of answer to it, response to it. The question is what limits, if any, should be applied to retention periods. It's not a question about how you retain data. It's just retention periods, and so I'd like to suggest we parking lot the encryption at rest issue. It's a good security issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. I would….

Paul Egerman – eScription – CEO
It's an excellent security issue to discuss, but we need to get through these sort of privacy issues also.

Carl Dvorak – Epic Systems – EVP
Paul, this is Carl, and I had a question on retention periods. As related to these intermediary organizations, HIOs retaining that data, won't they in many cases be required to retain it for legal purposes if there's a dispute or if there's a concern something wasn't done right? Wouldn't they need to be able to keep an archival copy to go back and track through the record of what happened? I just wonder if we're not really catching that element of what an individual business may need to retain from a records retention perspective for legal reasons.

Deven McGraw - Center for Democracy & Technology – Director
I actually think we have captured it, Carl. This is Deven. Your retention of data, it should only be as long as reasonably necessary to perform your functions and administrative activities related to those functions. To me, if there's a legitimate reason for you to keep it that's related to some of the functions that you describe, then that's captured under the recommendation. But what we want to avoid is people endlessly retaining. First of all, I don't want to assume that HIOs are retaining data at all.

Secondly, we don't want to leave an open ended policy related to data retention because that, to me, is dangerous, per Carol's earlier comments about collection of data for no clear purpose, particularly when that may actually be a copy of data. So I actually think we've got it covered under the language. There just isn't a one size fits all policy here. I don't know what other way we can say it other than as long as it's reasonably necessary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is a question. This is Dixie. Have we captured the – I know we've captured the for as long as. Have we captured for as much as?

Paul Egerman – eScription – CEO
I don't understand that question.

Deven McGraw - Center for Democracy & Technology – Director
I get it. Not just how long the data is retained, but what data gets retained.

Paul Egerman – eScription – CEO
Yes, but the question is retention period. In other words, the question itself is how long you retain the data.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I see.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
That's the question we're answering.

Deven McGraw - Center for Democracy & Technology – Director
Right, and we've already – we have arguably already addressed the question about use only, you know, specify the purpose, and collect and use only what you need to fulfill the function.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. You're right.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
This is Carol. I want to go back to one of the issues Dixie raised, and I agree that it's a meta issue, but somewhere in our discussion, the sort of conclusion that I'm coming to, listening to it, and I think the encryption issue is a good example of it, is that where collection and retention of information occurs, particularly a PHI of identifiably data, that we will find ourselves talking about higher levels of protection that are necessary. I just think it's a meta issue. It's fine to put it on the parking lot, but I just want to draw that conclusion out of the discussion.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
I made a note, and it's not, you know, it is actually something that we said in our set of recommendations to the policy committee in June is that where the greater exposure to PHI raises greater privacy concerns.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And also the security concerns.

Deven McGraw - Center for Democracy & Technology – Director
Right. Good point. I think we can move to the next slide.

Paul Egerman – eScription – CEO
This slide is transparency.

Deven McGraw - Center for Democracy & Technology – Director
Yes. There you go, Gayle.

Paul Egerman – eScription – CEO
Great issue.

Gayle Harrell – Florida – Former State Legislator
Let me tell you.

Paul Egerman – eScription – CEO
Here is our question. Should third party service providers disclose to their customers how they use and disclose information and their retention policies and procedures? I think we actually answered the last phrase just now. In this context customer refers to a provider that holds a patient record and contracts with a third party service provider. The third party service provider is also the same thing as what we called an intermediary, so we got a lot of terminology here, but basically this is a use and disclose. This is a question about transparency. The initial that's put forward is third party service providers should be contractually obligated to disclose to their customers how they use and disclose information in their retention policies and procedures.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. One of my favorite topics is transparency. I think you have got to absolutely define down to the Nth degree for that provider what's going to happen. They have to disclose exactly what's going to happen with that data. And also, I think then the provider has an obligation to let the patient know that as well.

Paul Egerman – eScription – CEO
Well, and we're going to get to that second part hopefully in a few minutes when we start talking about consent. But in the first part, Gayle, where you say that there's an obligation to disclose, how are you suggesting changing what's written here? In other words, what's written here adequate, or is something that needs to be added?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I just want to say that transparency and consent are two very different things. You need to be transparent separate and apart from whether or not there's a consent issue.

Gayle Harrell – Florida – Former State Legislator
Right.

Paul Egerman – eScription – CEO
I agree, but the transparency helps make decisions, right? In other words, the way I look at it is if you're asking somebody to make a decision about something, whatever it is, the more information they have, the better decision they can make.

Gayle Harrell – Florida – Former State Legislator

Paul, I have a question about contractually. Are we stating that they must do that within their business agreement, business associate agreement, or do they do that through that service provider contract?

Paul Egerman – eScription – CEO
I think it's one or the other. The actual form doesn't matter.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think, to make it parallel to the others, it does. In fact, to make these parallel to our other recommendations, I suggest we change the wording to the BA agreement between the service entity and the service provider should include full disclosure of how the service provider may use and disclose information and its retention policies and procedures.

Paul Egerman – eScription – CEO
It's a good question, although, to pick up on Deven's phrase, I think it's form over substance issue. The real issue is we want a contractual – the proposal is a contractual statement of basically everything they do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
My proposal is that we explicitly say business associate agreement.

Paul Egerman – eScription – CEO
Okay, so business associate and/or service agreement.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
To their customers, how they use and disclose information. Again, I want to get back to Gayle's comment. Is that an adequate response, Gayle? Is there something more that needs to be put here?

Gayle Harrell – Florida – Former State Legislator
I think, at this point, that's an adequate response if we get down to the patient level and then have the transparency also go to the patient.

Paul Egerman – eScription – CEO
Other comments on this? Is this an adequate response, or is there anything more we want to say about this?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
This is Adam. Do you also want to address deidentification and whether there are things that they do, such as selling deidentified information?

Deven McGraw - Center for Democracy & Technology – Director
It's broadly worded, right? It's how they use and disclose information.

Paul Egerman – eScription – CEO
First of all, could you repeat, Adam, what you just said?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Whether this should also include or also address deidentified information. For example, do they sell deidentified information?

Paul Egerman – eScription – CEO
Do you want to say, like, including without limitation, sale of deidentified data?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good comment.

Gayle Harrell – Florida – Former State Legislator
Good comment. Absolutely.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
….

Deven McGraw - Center for Democracy & Technology – Director
Yes. We have parking lot a bigger discussion of deidentified data, but Paul and I had a discussion about whether we thought we could open the door to having that be part of the transparency. I think the two of us were comfortable with raising, you know, at least putting that option out on the table with the hope that it didn't creep into more policy discussion related to deidentified data and was limited to this transparency aspect.

Paul Egerman – eScription – CEO
Yes, because the issue is, I think there's a concern that this occurs a lot and is not clearly visible, and so it makes sense that perhaps call it out.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
This is Wes. I have a really basic question where I'm either dumb, or it's ambiguous. But is this saying that it needs to disclose its policy on how it does and when it will do it, or it saying it has to disclose each disclosure?

Paul Egerman – eScription – CEO
…just the policy.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay. Does it say that? Or they will and disclose information?

Paul Egerman – eScription – CEO
…how they use … if we need to reword it, we can.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. All right.

Paul Egerman – eScription – CEO
The concept here, at least the way I pictured this is an HIO signs a contract with a provider and it's sort of like, I don't know, how the process….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. No, I understand….

Paul Egerman – eScription – CEO
And within the contact it says these are the things that we do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I understand what you're saying. I'm just not sure that the words say it, and if you look at that offline, it's fine with me.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Of course, it's always subject to the earlier recommendations about the limitations, but this is asking them to be transparent. I think this is asking them to be transparent about what they actually do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It's a really important principle, no question about that.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we've lost Adam's recommendation.

Paul Egerman – eScription – CEO
Yes. It hasn't been put in here yet.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Paul Egerman – eScription – CEO
Should be obligated to disclose … how they use and disclose. It says, how they sue and disclose information. We need … and you have a comment there. It should say including, without limitation, the sale of deidentified data.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I wouldn't use sale thought because it may not be a sale.

Paul Egerman – eScription – CEO
Including, without limitation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, deidentified data

Deven McGraw - Center for Democracy & Technology – Director
Deidentified data.

Paul Egerman – eScription – CEO
Use of deidentified data.

Deven McGraw - Center for Democracy & Technology – Director
Use and disclosure of deidentified data.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Actually, you don't even have to say use and disclosure because it was actually before the comma.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Including deidentified data.

Deven McGraw - Center for Democracy & Technology – Director
Right. Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Now this is all, of course, pursuant to the previous statements we've made and principles we've established as minimum necessary and all kinds of things of that sort, correct?

Deven McGraw - Center for Democracy & Technology – Director
That's right.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Right. And to clarify, for purposes of HIPAA, the business associate agreement has to specify under HIPAA whether or not you're going to deidentify, but then has no requirements that once it's deidentified that you provide any transparency as to what you're going to do with that information.

Paul Egerman – eScription – CEO
Yes, so now we've changed that sort of, or at least that's our proposal.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Would you repeat that, Adam? HIPAA requires that you – about the – when you deidentify?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
HIPAA requires that the business associate agreement specify all the uses and disclosures, which would include deidentifying the information, so the actual process of taking identifiable information and stripping it of identifiers, that's a use, and it's only permissible if the business associate agreement says that it's permissible. However, if your business associate agreement allows the business associate to deidentify the information, then what the business associate does with that deidentified information is completely outside of HIPAA. It does not have to be addressed in the business associate agreement at all.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I say—this is John Houston—that business associates don't uniformly agree with that, and I've gotten into a number of arguments with them about their use of deidentified data, so I think it's of value to put that on the table.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Okay, and I can provide you guidance that we have on that topic if you….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I understand, but I'm just telling you what the business associates like to say.

Paul Egerman – eScription – CEO

Yes. And so, John, when you say value to put on the table, was the way we did it responsive to your comment?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes. I just was coveting back on the previous comment. I'm sorry.

Paul Egerman – eScription – CEO
Yes. I think my experience is consistent with yours, so I think you're right. How do we feel about this? It's a really important question, and it looks like we've – are we coming to a consensus that what's written here is correct?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think this is our best one yet.

Paul Egerman – eScription – CEO
Have we got momentum here? This is really exciting.

Deven McGraw - Center for Democracy & Technology – Director
Let's just keep going.

Paul Egerman – eScription – CEO
I probably should just keep moving then because we'll go onto the next one. Not hearing any objection, I'm going to go onto the next one, and the next one is a very interesting question.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
The question is, are business associate agreements sufficient for insuring accountability?

Deven McGraw - Center for Democracy & Technology – Director
Related to third party service providers, not accountability across the board.

Paul Egerman – eScription – CEO
Yes, accountability of third party service providers (intermediaries). And there was a comment that recently proposed changes, as recently proposed – this was written – it's still – like still recently proposed, but written before the NPRM came out. Recently proposed changes to the HIPAA privacy rule strengthened the use of business associate agreements as tools for accountability. So it doesn't list any options, although I could suggest two options.

Deven McGraw - Center for Democracy & Technology – Director
Yes and no.

Paul Egerman – eScription – CEO
One would be yes, and the other one would be no. Let's assume that those are our two options to get started with this question. Are business associate agreements sufficient for insuring accountability? Does anybody want to say yes?

Deven McGraw - Center for Democracy & Technology – Director
I think it's a mixed bag. This is Deven. I think there was some significant strengthening, especially with

respect to defining downstream subcontractors who have routine access to PHI by virtue of their contracts with business associates. That coverage, I think, is an important proposed provision. I think the one thing that I'm still a little worried about is the imbalance of power often between the entity that's a business associate and some of the smaller, less economically resourced covered entities. I'm not sure how to resolve that. I think my own opinion, obviously, since I'm saying it, is that there were great strides made in the proposed rule that we may want to expressly acknowledge given that it's a comment period. But I still worry a bit about what's a small provider to do if they have concerns about uses of data that are being proposed by a particular HIO, and they sort of either have to sign or go it on their own.

Paul Egerman – eScription – CEO
Is your answer yes, pretty much? I'm trying to understand.

Deven McGraw - Center for Democracy & Technology – Director
It would be yes with caveats.

Paul Egerman – eScription – CEO
Yes, kind of.

Gayle Harrell – Florida – Former State Legislator
This … address that too. I think mine is a no, but.

Paul Egerman – eScription – CEO
No, but, okay.

Gayle Harrell – Florida – Former State Legislator
A no, but. I have a great deal of concern that there is that imbalance of power, and I think you're going to have some governance issues that I don't know where that conversation is to be placed in how we discuss things, but I think there's going to have to be some governance of these third party intermediaries or HIOs or whatever that establishes some parameters and some oversight at maybe the state level that is going to require them to do something under penalty of law. I don't know how we get there, but I have a real significant problem with some of the structures out there that I see developing, and also what they are going to really say it's my way or the highway to small providers.

Paul Egerman – eScription – CEO
Yes, so those. Any other comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I would second Gayle's concerns. I think there are some near monopolies in the connectivity space, and some of the meaningful use requirements make it more or less obligatory that you use those services, and some of those services may have provisions that you're not comfortable with, but there's not a whole lot you can do about it as a small provider.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. I don't think it's necessarily even a small provider phenomena. We deal with this with certain large business associates today, not just in this space. But I think, as these form, I mean, it's probably very difficult for business associates to be able to handle the nuances that any provider gives it. If you have hundreds upon hundreds, if not thousands of business associate agreements, to say you're going to agree to some nuance to a standard form might frankly say, yes, I'll agree to it. But then the realization is that they may never be able to comply because how do they track all of those differences? There's got to be a better model for insuring that a common business associate agreement provides a

reasonable, objective level of performance on behalf of the business associate and one that I think covered entities can also feel comfortable with.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I thought Gayle was going to say this. Since she didn't, I will. It depends on accountability to whom. And I think that it provides, the BA provides more accountability to a covered entity than it does to a consumer, and I think, at the consumer level, it really doesn't do that at all. So I would ask accountability for to whom.

Paul Egerman – eScription – CEO
I have to say, on this issue, I tend to agree with what Gayle is saying. Having been a business associate, one of the things I know is you sign the agreement, but then nobody really ever checks to make sure you're doing what it says. Like we just talked about, like retention periods, which I know is a significant issue. But absolutely nobody ever checks to make sure that you really are doing what you say you're going to be doing with the retention period. And so you could, and these are issues that, when you get to governance, there are ways you can solve them. You can require HIOs to do annual audits to include an audit of their retention period, but it has to be done by a third party auditor. That would be the kind of thing that I think – I don't know if that's what people mean by accountability, or if that's just an issue of compliance. But it would seem to me that you need more than just the agreement in place to make sure that the stuff happens the way it's supposed to happen.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We need to see how HITECH plays out because HITECH significantly strengthened the oversight of business associate, so probably all of your experiences before HITECH, you know, certainly before the NPRM that this came out.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I think that's right. This is Deven. But I appreciate the comments, and I think that we can both praise the rules treatment of BAs and clarifications around BA appropriate access to data and the clarification that it extends to subcontractors as well, but also acknowledge that for a collection of reasons, balance of power, maybe less resources available for oversight, there needs to be something else here from a governance standpoint, and then take that up with some more rigor when we get to the governance question.

Paul Egerman – eScription – CEO
It sounds to me like the answer that we're coming to, to this question, is sort of a merger of the yes, kind of, with the no, but, where we say business associate agreements with the proposed changes are an important step forward, but an additional governance model needs to be established.

Gayle Harrell – Florida – Former State Legislator
That governance has to, as Dixie said, and I'm glad she picked up on it, so that there is that accountability, and the patient can feel secure because … confidence that the patient is going to have in these third party intermediaries, we're going to have a major issue of all this.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. I'm all for governance.

Deven McGraw - Center for Democracy & Technology – Director
We're stealing your thunder, John.

Paul Egerman – eScription – CEO
Yes. We thought that you would like our response to this question, John.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Thank you so much.

Paul Egerman – eScription – CEO
But you've influenced us here. Basically you're right. The more you think about it, we've got to do this. The way I propose answering this question is to say business associate agreements are an important step in this process, and the proposals to strengthen them are considered to be very positive, but additional governance procedures needs to be established.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm leery of the lumping of terms in governance procedures because I think that word has a lot of different connotations, and it's not specific enough. Going back to FIPs, I would suggest that there are three principles that apply here, which is oversight, accountability, and enforcement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Say that again, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. I'm leery of lumping everything that we're discussing into something called governance because people interpret that very differently. Going back to FIPs, Fair Information Principles, there are really three buckets here that apply. One is oversight. What is the oversight mechanism, which gets at some of the issues that Paul was raising around audit; accountability, which is obvious; and enforcement.

Gayle Harrell – Florida – Former State Legislator
Yes. You have to have all three.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I agree. I lump those in terms of governance, but if you want to put those in parentheses maybe.

Gayle Harrell – Florida – Former State Legislator
It's the definition, really.

Paul Egerman – eScription – CEO
That's a valuable comment, Carol. How do you suggest we respond to this question then based on…?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm suggesting replacing the term governance because governance to some people implies the sort of administrative approach to the way an organization is run, and I don't think that that's what we're talking about. It has other connotations. I'm suggesting we stick with the standard sort of FIPs terms and use those three words instead of governance.

Paul Egerman – eScription – CEO
Excellent comment.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
This is John Houston. I would prefer it would be explanatory rather than in place of. I still like the term governance because it may include other things as well. But I think you would, at a minimum, want to handle those three things that Carol talked about.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Let's do the Carol things and say sometimes referred to as governance or often referred to as governance or referred to by John Houston as governance. We can have all those terms in there, but it sounds like we're all comfortable with the concept that the three FIPs, the triangle needs to be expressed so that it's clear that that's what we mean.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – eScription – CEO
So our answer is the … by itself is not adequate. That the governance issues of oversight, accountability, and enforcement need to be addressed.

Deven McGraw - Center for Democracy & Technology – Director
Yes. There are two pieces. One is that she said it, which was saying that there had been some, you know, I can't remember.

Paul Egerman – eScription – CEO
You want me to do the more diplomatic.

Deven McGraw - Center for Democracy & Technology – Director
Yes. There were two pieces of it, to acknowledge the….

Paul Egerman – eScription – CEO
While significant forward strides have been made, the business associate agreement, the additional governance issues of oversight, accountability, and enforcement need to be addressed.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. I would just suggest that one of the values of having those three terms is that it becomes very clear that the BA is merely a mechanism of potential enforcement. But it is not a mechanism of oversight or accountability, necessarily. That's the value in having those three terms broken out. It forces you to think about all three.

Paul Egerman – eScription – CEO
Yes. While significant strides have been made, business associate agreements by itself or by themselves are not sufficient, and the governance issues of oversight and accountability and endorsed enforcement need to be addressed. And we'll do the spelling later.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
As this is coming out on the screen, are people comfortable with this? Is this an adequate response? Does anybody have anything they want to add or disagree with?

Gayle Harrell – Florida – Former State Legislator
It looks good to me.

Paul Egerman – eScription – CEO
Any other comments? That's terrific because, believe it or not, we've completed all nine of our questions.

Deven McGraw - Center for Democracy & Technology – Director
Yes, and we're going to – so….

Paul Egerman – eScription – CEO
Yes. Maybe that 10:00 press release was really for us because they probably finished their meaningful use thing, and now they're announcing that we actually got through all of our questions, and now we can start to talk about something very interesting….

Deven McGraw - Center for Democracy & Technology – Director
One of the things that we will do, as Paul mentioned earlier in the call, is to pull these recommendations that we've made over the last two calls into a complete set for folks to take a look at. I think, ideally, in between our meetings, our next one is on Friday, and that Friday call is our last one before the policy committee meeting on the 21st, and so if we can sort of get those wordsmithed and in order and put the final blessing on them on Friday's call, that would be terrific. Right? Am I misstating, Paul?

Paul Egerman – eScription – CEO
That's correct. What you see on your screen, it says next meeting is July 13th. That's actually the next meeting is July 16th. We're going to get all this material to you, but also as you see correctly on your screen, what we're really going to focus on is consumer choice and consent. And since we have time in today's call, what we'd like to do is get started with that discussion. And so, in getting started with that discussion, we've put together this list of six questions that we wanted to answer.

I think the first part is to explain the questions and also explain what we mean by consumer choice. What we're talking about by consumer choice right now is sort of like whether or not to play the game, in other words, whether or not to participate in the exchange. We're not talking about once you participate, who gets access to what data. That's going to come later. This is, are you playing? Is a particular individual going to be involved in this entire process?

The six questions that you see on the screen, the first one is what are the factors or circumstances that would trigger the need to provide patients with choice. The second one is, if choice is needed, what model should be followed? What model of choice as opposed to what model of HIE. The third one is interesting. Should provides have a choice as to whether they participate in an HIE? The fourth one is also interesting. Who is going to educate consumers about this whole process? The fifth is how and by whom consent should be obtained and managed. The last one is the durability of the consent.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have a question. This is Dixie Baker. A lot of the sort of initial question is how much transparency they have, how much they know. Is transparency a separate topic, or is that included in our consideration of these bullets?

Paul Egerman – eScription – CEO
Didn't we answer the transparency question a little bit in terms of what the…?

Deven McGraw - Center for Democracy & Technology – Director

No, we only answered it for providers.

Paul Egerman – eScription – CEO
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It was put in the parking lot.

Deven McGraw - Center for Democracy & Technology – Director
Yes. We have a sort of patient issues, for lack of a better way to phrase it, topic that's coming up at a later hearing, but I think folks can sort of toss out, for example, assumptions that in fact there's some degree of – that consumers, at a minimum, have transparency of how their data is exchanged, not just what their rights are under HIPAA, but what actually happens.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That's what….

Paul Egerman – eScription – CEO
Yes. We do also have the fourth question is who should educate consumers about consent and health information exchange. That sort of implies that there's something, that there's some level of transparency because obviously there's an educational process involved.

Deven McGraw - Center for Democracy & Technology – Director
Right. It's just not expressly stated, so certainly….

Paul Egerman – eScription – CEO
That's a good comment, Dixie, and we should have that as an assumption. I guess the first issue is, before we dive into these question is, does anybody have any comment on the questions themselves? Are these the right questions that we should be asking?

Gayle Harrell – Florida – Former State Legislator
Are you suggesting that we do put that comment that we combine that transparency for the patient? I would put that as really either make that very clear within the question that who should educate, but also asserting that the patient has to have the knowledge and that the transparency is there for the patient.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And what information they really have access to.

Gayle Harrell – Florida – Former State Legislator
Correct. What exactly is that HIE going to do with my information?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Is there a significance in using HIE rather than HIO here?

Deven McGraw - Center for Democracy & Technology – Director
It was actually purposeful, Wes. This is Deven. I wanted to see if we could, for the first question in particular, think about certain factors that may be present in any time of model of exchange that trigger

the need to provide patients with additional choice, and all of this is beyond what current law already requires, which is another assumption that we sort of didn't state expressly here, but that we've certainly talked about in previous larger privacy and security workgroup conversations, which is that the assumption is that where the law requires authorization, we're not disturbing or overriding that. We're thinking about layers on top of that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That could be state or federal.

Deven McGraw - Center for Democracy & Technology – Director
Right. State or federal, that's right. Folks know the general rule with respect to HIPAA, there is authorization specifically required for identifiable substance abuse treatment information at the federal level. School facilities have a different set of laws under FERPA, and then the state laws. We're assuming that all of those exist.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If a hospital contracts with a third party to deliver its reports to providers, is that an HIE? To me, I'm struggling with this issue of whether every business associate that transmits data anywhere except to and back to the provider client becomes an HIE.

Paul Egerman – eScription – CEO
Yes. Let's go back to basics, Wes. When we're talking about HIEs here, we're going back to issues of coordination of care and treatment of patients. So this is really what we're – that's a primary issue that we're talking about, although I suppose we're also talking about quality reporting and the public health thing. But it's really predominantly coordination of care and treatment, and it's the exchange of information from one healthcare entity to another entity. If we have John Houston on from UPMC that … exchange from UPMC to say, I don't know, Kaiser or perhaps even to a private practice physician in the city of Pittsburgh that was just outside of the UPMC boundary entity boundary, so it's really an exchange of health information from one place to another. It does not include a business associate agreement that a hospital might have with an EHR vendor, for example. That's not exchange. That's a different agreement.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm not trying to be too picky here, except sometimes the edge case helps you understand.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If in fact a firm came to UPMC and said send us all of the lab results from your labs, and we will deliver them to physicians in the area, so we won't retain that. We won't do any other services. You can't look up the data, etc. That's still a health information exchange by….

Paul Egerman – eScription – CEO
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks.

Paul Egerman – eScription – CEO

Yes, that would be, or even a more simpler thing is a physician contracts with a national laboratory for its laboratory results and sends its orders to the lab, and the lab sends the results back. That's health information exchange.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Why would that be? That's between two.

Paul Egerman – eScription – CEO
It's still an exchange.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, okay, so now that's exchange as a verb, but not exchange as a noun. That is, there's no third party.

Paul Egerman – eScription – CEO
There's no third party, but you still have an exchange going on there. It's a directed exchange, but you still have an exchange.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So we're including in discussing consumer choice and consent, we are saying that we're asking the question whether every data relationship between two providers is subject to choice and consent.

Paul Egerman – eScription – CEO
Yes. It asks the question a little bit differently. What are the circumstances that do cause you to trigger consent?

Deven McGraw - Center for Democracy & Technology – Director
Right. In other words….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But the consequences of our answer could be as far reaching as I chose to emphasize in my….

Paul Egerman – eScription – CEO
You could.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right. Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes, it could potentially. This is Deven. So just to give an example, I've seen materials from one state where the line that they're drawing is based on whether the exchange is electronic or not, regardless of model, so that if a provider is sending, like in what we've called the directed exchange model, a provider is electronically sending data from one provider to another, but that's an electronic exchange that requires some choice, even in circumstances where there's not an HIO used. The provider is vetting independently the decision to send the data or is sending it on his or her own initiative. If it's electronic, consent is required, and if it's not, it's not. Now I happen to think that that's a sort of odd way to draw it, but I don't think Paul and I wanted to leave that off the table necessarily.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
No, I understand why it's important to get the outside of the coral. When you say electronic, under that definition, a fax would not be electronic, right?

Deven McGraw - Center for Democracy & Technology – Director
That's correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right.

Deven McGraw - Center for Democracy & Technology – Director
Well, that's under the particular state that I'm talking about.

Paul Egerman – eScription – CEO
It sure seems electronic to me, Wes, but it's a good question.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, no. I think we go all the way back into early HIPAA to find that interesting distinction.

Paul Egerman – eScription – CEO
But you ask a good question, Wes, so the first part, the first question I should ask is are the questions understood? Do people understand what the questions … make sense?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
This is Carol. I'm struggling here. I don't know how to articulate it yet, but let me just raise one issue first, which is, going back to the call. God, these calls, they're so long, and there are so many of them, they bleed into each other. But whatever call we had earlier last week about the control over the information, in other words, who is responding to the exchange definitely applies here for me because if it is the provider and presumably along with the patient, that raises different issues than if it's a third party who has access to the data and is deciding whether or not to exchange the information.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
That's right. Although, it's interesting you raise that, Carol, because in some sense, I view what you just said as one of the possible answers to question number one.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
In other words, the issue about who has control over the data might be an issue that would trigger the need for choice or for consumer participation.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right. I agree with that. The assumption here is that if the provider is making the decision, presumably along with the patient, that that fits into a different category of issues. The provider may still want to get the patient's consent. In other words, when you go and ask a provider in the analog world for your records to be sent to another doctor, they still make you sign something. And that's even when the patient asks, so I guess what I'm trying to raise here is that if that kind of safeguard is in place, in other words, the provider is making the decision with the patient, it's a very different construct than if the

information resides elsewhere and some third party that does not have a relationship with the patient, and I think that is the key, is making the decision.

Paul Egerman – eScription – CEO
Okay. You raise a good issue. It's a variation of the issue that Dixie raised. The basic assumption is that this is a decision that's being made between a patient and his or her provider.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Correct.

Paul Egerman – eScription – CEO
…clinician. Correct?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I don't know. I thought Carol just did a good job of articulating one of the important factors for number one.

Deven McGraw - Center for Democracy & Technology – Director
I thought so too.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, right. I think that the question can come up exactly as Carol said. Where there is a third party holding the data, and we're not trying to exclude that from consideration here.

Paul Egerman – eScription – CEO
Do we want to just launch ourselves into number one?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
You asked about some questions on the questions first, if we can go back to that, so I can see the questions, then….

Deven McGraw - Center for Democracy & Technology – Director
Yes. I can't see them either.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Somebody just took the questions off the screen.

Paul Egerman – eScription – CEO
It'll come up in a minute. I think I have a faster computer or something.

Deven McGraw - Center for Democracy & Technology – Director
Yes, you do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I see. There's a different format. These are the same questions, but they're in a Word document instead of in the PowerPoint we were looking at.

Paul Egerman – eScription – CEO
This is a technical test, Wes. You notice you passed.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. You want me to read all the signs when I'm going down the street in Las Vegas too? The third question, I just simply don't understand. The notion that they might not have a choice is kind of hard to get my hands or my thoughts around. And the sixth question probably implies a related question, which is what is the treatment of data that might have been retained before consent was changed or something like that.

Paul Egerman – eScription – CEO
The first one you had was the third question. That came up in our discussions as unclear that in some situations that providers could just choose not to participate at all. It came from a presentation I saw of a health information exchange actually in the state of Utah where the person running it said that participation was assumed to be mandatory because it was a government funded project. It was an interesting statement to make. And so we wanted to clarify that issue. The issue that you raising for question six is a great followup question, which is if you give consent and then you withdraw it, what happens to the data.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks.

Paul Egerman – eScription – CEO
Good comments. Are there other comments about the questions?

Rachel Block – New York eHealth Collaborative – Executive Director
This is Rachel. Just a factual update on durability: I think many of you probably saw that SAMHSA finally issued their long awaited guidance in the form of a frequently asked questions document.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
What agency was that?

Rachel Block – New York eHealth Collaborative – Executive Director
SAMHSA, substance abuse, that put some specific parameters around the issue of durability, so I'm not making a proposal. I'm just letting you know that that might be something that we want to put on the table just for information for the group.

Deven McGraw - Center for Democracy & Technology – Director
Right, to take a look at.

Paul Egerman – eScription – CEO
That's very helpful, Rachel.

Deven McGraw - Center for Democracy & Technology – Director
Thank you. I haven't had a chance to read those yet. You're just reminding me.

Rachel Block – New York eHealth Collaborative – Executive Director
Yes. It's a little awkward because what they basically said was you can't have infinite durability, so you have to address durability in some way, but it could be that I give you consent for the rest of my life or

something like that, which I don't know. That doesn't really, you know, it's just a little bit weird. But anyway, it's there for people to take a look at.

Paul Egerman – eScription – CEO
Great. Other comments about the questions themselves? Not hearing any comments, I'm wondering, Deven, if we should go ahead.

Deven McGraw - Center for Democracy & Technology – Director
I think we might be able to get some more of the factors in number one.

Paul Egerman – eScription – CEO
Yes. I think that would be a good discussion to have. That would give us a running start on this thing for Friday.

Deven McGraw - Center for Democracy & Technology – Director
And ask people to continue to give us feedback in the interim. I think this is typically an issue that people have some thoughts about, and one of the things I was hoping would happen with the factors decision is to sort of tease out those points of discomfort where people feel as though even notwithstanding whatever rules we might put around various electronic exchange and maybe even specific to various types of exchange, we would still want patients to have some choice where certain factors are present. Carol started with who has control over the data is another one whether the data is aggregated.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I have a question about that in thinking a bit more about it. The conversation at the beginning sort of defining an HIE. If in fact the exchange is just from one provider to another, getting consent would run against what HIPAA says.

Paul Egerman – eScription – CEO
We've already dealt, I think, with that issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I didn't hear. I thought you included that as a possibility.

Paul Egerman – eScription – CEO
I just included that definition of an HIE.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So if we include--?

Deven McGraw - Center for Democracy & Technology – Director
Well, except, I'm not….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If that's included in the definition of an HIE—

Deven McGraw - Center for Democracy & Technology – Director
We specifically, I thought, Paul, did not use the noun form in number one. We were not an HIE, but HIE.

Paul Egerman – eScription – CEO
Yes.

Deven McGraw - Center for Democracy & Technology – Director
And so what aspects of models of exchange as a verb are ones that trigger the need to provide patients with some additional choice as to whether their data is subject to exchange with that characteristic, for lack of a better way to frame it. It's a little bit awkward.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If that's a verb, then the biggest factor is whether it's for treatment, payment, or healthcare operations because the patient doesn't have consent if it's for those purposes.

Deven McGraw - Center for Democracy & Technology – Director
I know, but the purpose of this, Dixie, is not just to state what current law is, but to think about assuming current law, whether we want to put some additional requirements on top of that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Current law is the baseline, even though….

Deven McGraw - Center for Democracy & Technology – Director
That's the baseline, right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Even though we've extended HI … okay. Got it.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
This is Adam. Just to clarify one point. I don't want to go too far down this road, but HIPAA does actually have explicit provisions for voluntary consent.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
It promotes that a provider should feel free to seek voluntary consent for treatment, payment, and healthcare operations, so I don't want to have anything suggesting HIPAA is an obstacle to voluntary consent like this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
We have so far, who has control over the data, whether the data are aggregated, so the correct … use of the word data.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The sensitivity of the data.

Paul Egerman – eScription – CEO
Yes, how sensitive data is handled.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. I'll throw another one out. It's a little slippery, but we wrestled with this in an original blog post that Wes and I did on simple interoperability trying to make a distinction about data exchange for an existing consented episode of care versus data that was aggregated for future, as yet unconsented episodes of care. So it's a little bit of the who can control the data, but it's also are you actually building a collection of data that could become useful in the future, should someone need it?

Deven McGraw - Center for Democracy & Technology – Director
It sounds like you had consent in both variations of that model.

Paul Egerman – eScription – CEO
Yes, but there's another way of saying what you just said, David, is whether or not data is retained for future use.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, by someone else's, by a third party. I mean, I think it takes two. The physician is going to retain it in his own record, of course. He's required to, and you wish him to. But is he contributing that data to a third party for future uses that may in fact be outside the current consent and treatment?

Paul Egerman – eScription – CEO
I just wonder if a better way to write this sort of fourth bullet would be to see whether a third party retains data for future use.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I just want to say, this is a very slippery slope because future uses is a very tempting construct because it leads to two things. One is, well, let me just collect everything because I might have a future use. And the second is blanket consent where you basically ask the person to consent to anything and everything. I want to make sure that we understand that it's very important to put upstream constraints on those temptations because it is truly what can lead to unnecessary exposure.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Carol, that's why I was raising this. I think this is one of those circumstances, which does require consent.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree.

Deven McGraw - Center for Democracy & Technology – Director
Right, but I think Carol's point is related to some of the earlier statements that we made about not necessarily relying just on the patients to curb unnecessary retention and collection of data. I mean, we had already said that based on the purpose specification, collection, and use limitations that as a core principle, irregardless of patient consent, that those ought to be limited. That doesn't mean that it's not worth labeling, you know, setting forth here as an issue to talk about in terms of consent, but keeping in mind that I think we've arguably already said that we wouldn't just leave it up to patients about whether their data gets aggregated for future use or not.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That we would not leave it up to patients?

Deven McGraw - Center for Democracy & Technology – Director
No, that we would not necessarily. I mean, I think what I'm trying to avoid here is allowing entities to use patient consent as a vehicle to do an end run around adherence to basic steps, fair information practices about how they collect and use data. My concern about this is because patients far too often don't read or understand consent statements, and it's essentially putting the burden on the patient to set the privacy parameters of data use and exchange models, which I want to avoid. Ideally, I think, we give patients choice, but we don't imbue it with all of our expectations for privacy protection.

Paul Egerman – eScription – CEO
This is Paul. What you just said about patient choice is interesting, Deven. I was just thinking. Last week, after one of our calls, I had a very minor surgical procedure, and I ended up signing two consent documents. The first one was a two-page document about the surgery that sort of said all surgeries have benefits, and they also have risks. And without describing any of the benefits, it then had like three paragraphs of everything bad that could happen.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Informed consent, right?

Paul Egerman – eScription – CEO
It was informed consent, right. But it was clearly boilerplate. They used it for like anything. And the second document was that I had to acknowledge that a picture of the site would be placed in my medical record. When you're a patient, and you're partially dressed, you sign these things, and it's frustrated in terms of what they really say. It's just an observation, perhaps not all that helpful, but maybe it does go back to some of even Carol's statements. We throw all this stuff in front of patients, and they just sort of grit their teeth and sign it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. I think it reinforces both Carol and Deven. After all, HIPAA consent is a Hobson's choice anyway. You can … we aren't going to treat you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I think you have to – you know, maybe we want language in there about avoiding coercive consent, but I think at some point you have to assume an intelligent and thoughtful consentor and figure out what your policies are. In other words, the person who wants to control their record and understand their choices, what are they allowed to do. Then, as a fall back, what do you do to prevent coercive consent or whatever the right term is for the patient…?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

Paul Egerman – eScription – CEO
Those are good comments.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
This is Carol. If I just might offer, I don't think our discussion is meant to say intent is not important. It is rather, and this goes back to FIPs, right? Individual notice and control is one principle, but it is nested in the other. I think Deven made the point earlier, which is, consent is more meaningful if it is buttressed by the other policies and protections like use limitation, you know, all the ones we've been discussing today: oversight, accountability, enforcement. The issue I think that bears strong consideration is to make sure

that those other requirements are in place so that – I think … is a good word – so that consent doesn't be kind of a way out. The patient consented, so we….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm assuming that, you know, take the edge case is the patient who decides they don't want any sharing to occur. What control did they have? What's the extent to which the patient has choice here? Then work from there out to how do we avoid abuses of that? You can't allow; you can't disallow sharing because some abuse might occur, so we have to figure out, how do you control sharing and then worry about how to prevent abuses. I certainly agree, those principles should be always extant, but some patients may wish to share nothing, and others may wish to share everything.

Paul Egerman – eScription – CEO
Those are all good comments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. That third bullet, what I said was how sensitive the data are, not how sensitive data are handled. I also, I'm not sure whether it belongs in this, but this whole idea of how much visibility they will have in what happens to it in the future also is a factor. They might give their consent for something to go into a repository, let's say, as long as they know that they'll be advised whenever it's used. Maybe you can help me phrase that correctly.

Deven McGraw - Center for Democracy & Technology – Director
But since consent, you have consent at the original branch of authority to use that information, doesn't your question, Dixie, go more to the form of consent versus whether consent is or isn't required to be obtained?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'll give you this example. I might, and this is common, a commonplace, actually. Patients may consent to have their data be considered for use in research with the understanding that if their data are to be used for particular research study, they are notified of it. In fact, they are, by law, I think they have to, well, except there's … flavor. But they still would want to be notified if their data are used in a particular….

Paul Egerman – eScription – CEO
One of the circumstances I think you just mentioned that would be use of data for purposes other than treatment. Is that what you're saying?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. I'm saying that you might – it relates to David's on aggregation. You may consent to having your data in an aggregated repository under the condition that if the data are actually being used for other purposes, you'd be notified.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I'd like to also say, where does the granularity consent come in?

Paul Egerman – eScription – CEO
That's a good question, Gayle. Where we are handling this issue right now, rightly or wrongly, maybe wrongly, is to say the first question is sort of like to play at all. In other words, whether or not you're going to participate at all. Then we're going to have a discussion about, well, what data and who has access to what data once you decide to participate.

Deven McGraw - Center for Democracy & Technology – Director
Right. We're attempting to bifurcate this with the full knowledge that that's not necessarily an easy thing to do, but we want to at least get some parameters out there for when circumstances when choice ought to be beyond what's required in current law, and then think about the granularity at which that can get exercised separately, again, acknowledging, not always easy to separate.

Paul Egerman – eScription – CEO
Getting back to the factors and circumstances.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Mine wasn't recorded yet.

Deven McGraw - Center for Democracy & Technology – Director
I have to admit, I mean, I'm struggling, Dixie, with how to record it because you've already got consent to the aggregation, and we've got the primary question is not how choice gets exercised, but whether or not you get it in the first place.

Paul Egerman – eScription – CEO
Maybe there's a way I can think of to respond to what Dixie is saying. First, what I would say is one of the factors ought to be who has access to the data. In other words, one way to think about this is instead of saying the data, think about it as this is my data. Who has access to my data? I would think that that would be a factor that you would want to know.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I guess I was piggybacking on David's, as I said before. He says unspecified future use.

Paul Egerman – eScription – CEO
I understand. I was going to get to that, Dixie. If you first have the question, who has access to the data, the next issue might be either what controls or what notifications are available, or people who access the data, or accesses and use.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. This is Carol again. I'm worried about this conversation because I think we are assuming all making may be different assumptions about what the data are. The data may be some portion of my medical record. It may be just my demographics which are retained by the HIE. The answer to this will really depend on what's at risk, what's being exposed, and I'm struggling with trying to have this conversation about every possible permutation of what that data is.

Paul Egerman – eScription – CEO
We do have something called how sensitive the data are.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director

Right, but maybe this, Carol, goes to a level of identifiability or extent of data, whereas sensitivity may be, you know, is it in terms of the health data? Is it mental health records? Is it HIV records? In Carol's example, is there health information at all, or is it just purely demographic data? Is it identifiable? That's sort of….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I put identifiability as a separate bullet. That's an important one.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I agree that identifiability is important, although it is covered by a lot of the HIPAA stuff. I wonder, Carol. Are you concerned about some of the architecture choices and whether those have bearing on…?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Look, I definitely think architecture and what's stored and where it's stored has bearing on policy. Let me start there. But what I am suggesting is really an issue of risk. If data is aggregated by an HIE, and it's only demographic data, and the data are breached, however they're breached, that's a different kind of risk than if it's both my demographic information and my medical/clinical information. They're just different levels of risk there. And how much information, exactly what – you know, all these things bear on risk level.

Paul Egerman – eScription – CEO
Sure, but don't we have at least some of those? We have what is the data being exposed, how sensitive the data are?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But she's right. She's putting them together that you may have something independent. The data itself independent of other data may not be all that sensitive, but the aggregate for you is more sensitive. She's right. We haven't really captured the whole risk index.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I agree. If your provider said, you know, I use Facebook to share your medical record, you might opt out.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you might.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But I think the core question is that one about who has control so that regardless of the architecture, assuming that it is a secure architecture, I mean, just say that's incredibly important, but for the moment, put that on the table and say, assume it's a secure architecture. It doesn't really matter where the data is stored as much as it matters who has control to access it. That was the only point I was saying was that control trumps architecture.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Sort of.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Well, architecture implies control, right?

Deven McGraw - Center for Democracy & Technology – Director
I think they are part and parcel.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and there is no such thing as a secure architecture. There are levels of security.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, of course, so sufficiently secure. In other words, I'm getting at the thing like the difference between a record locator service and a central repository from a control point of view, there's not that much difference. If someone has access to the record, they can get the record.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No, it's two separate issues. With control, if the provider and the patient are in the decision making role of deciding whether and when to share information, it's different than if a third party is, right? We discussed that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that's control, who gets to decide.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right, but the issue of what is collected and aggregated by a third party is a completely different issue because if I get access to demographic information only because I breached the HIE or O or whatever we're talking about.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So you're talking about breach and risk.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I know. That's a different level of exposure than if all of my information is aggregated, regardless of who controls it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I agree, and that's the breach and the risk side of things, which is a different issue than consent.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
We agree that we have to decide how we handle this when things go right and what preparation we make for the possibility of things going wrong, such as a breach, such as a subpoena. There are a number of issues….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Not that I would say a subpoena was wrong, but I just wanted to reflect back on our hearing a couple weeks ago and say that another item or another issue related to consumer choice consent is the frequent, is the complexity of the decisions consumers might have to make and the frequency with which they might have to make them. VA talked about the patient going to their privacy council to work on their statement of how they wanted to share their data. It struck me that that is a variable we just have to consider.

Paul Egerman – eScription – CEO
These are good discussions. I'm also keeping track of the time because we also want to make sure that we leave some time for public comment.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would like….

Paul Egerman – eScription – CEO
I'm sorry, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Just so we don't lose Carol's comment, I'd just like to suggest we just put on their perceived risk.

Paul Egerman – eScription – CEO
Here's what I was going to suggest that we do. This is a great discussion. What I'd like to suggest we do is we're going to take this Word document and circulate it by e-mail to everybody and ask you, before Friday, to add to first for question one, what other factors or circumstances you think should be added. But as you put that into the document to send it to e-mail to all the other members of the tiger team, so we can have a discussion on this through e-mail, the same way we did the public health discussion, because I thought it was an excellent discussion, and so that could be a way that we could continue to discuss this question number one.

Now question number two talks about the model for choice. Maybe I'm assuming something that's wrong. I assume this is a question of opt in or opt out. Is that what this is when it talks about model?

Deven McGraw - Center for Democracy & Technology – Director
I think so, yes.

Paul Egerman – eScription – CEO
Okay. And so the other thing I'd like to suggest as homework would be when you go through this Word document would be to write up your opinion on question number two, which is opt in, opt out, and why you choose one or the other, or if you think that there's another choice, or you think that's not the right issue for us to address.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'd like to just say, I think that's an impossible exercise because the answer will depend on opting in or opting out, of what, for what purpose, you know, under what conditions. I don't know how to do that.

Paul Egerman – eScription – CEO
So you don't think that's a good question for us to ask at all.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No, not unless we are willing to define the answers to all those questions, and that includes architectural questions, where the data is, who has control over it. If we wanted to find one model, yes, you can get there. But I don't know how to answer that in the abstract.

Paul Egerman – eScription – CEO
I think that by itself there is an answer to the question, so that would be your way to answer the question, and if people agree, that would be fine. But if we could get responses on at least the first two questions,

and if people want to respond to the others, that would be terrific. The goal is to get people to have some discussion and express opinions like the one Carol just expressed, and so that when we have our meeting on Friday, that we can make some more progress on these issues.

Judy Faulkner – Epic Systems – Founder
Paul, this is Judy. A different view on this, and I wanted to know if you think this should belong in here or not. I recently did a click through on my phone of a consent that they needed for me, and it was 94 screens long. It said I had to read the whole thing and then consent yes or no. Obviously that's ridiculous. So my question is, when we get to some of the personal health records that are not covered by HIPAA, do we have any say in the consent for personal health information and how that's done there? And having read some of them, and I read this in blogs as well, are very complicated to figure out whether they're saying they're going to do anything with your information or not, so that's one confusing part. The other thing is many screens long is hard. Is that included in what we're talking about here or not?

Paul Egerman – eScription – CEO
I think you raised a number of issues there, Judy. Certainly as part of your answer to question number two … choices needed, what models should be followed, I think it was intended to be opt in versus opt out. That would be a good place for you to make an observation that the consent process should be terse, should be simple, and shouldn't be like signing a home mortgage or something.

Deven McGraw - Center for Democracy & Technology – Director
Yes. But with respect to PHRs….

Paul Egerman – eScription – CEO
That's a separate topic.

Deven McGraw - Center for Democracy & Technology – Director
That's a separate topic.

Judy Faulkner – Epic Systems – Founder
Yes, that's what I was wondering. Does that come at all or not?

Paul Egerman – eScription – CEO
Is what I'm suggesting, Deven, for – I don't know if homework is the right…?

Deven McGraw - Center for Democracy & Technology – Director
Yes, I think so. Although, I would hope that, and I'm going to send an initial e-mail to everyone, including the MITRE team because some of the e-mail communications haven't, you know, I think people used best efforts to include everybody, but they've been missing some folks. So if you reply, use the e-mail that I'll send immediately after this call to do your replying, and then we'll make sure that it gets to everybody. That includes the MITRE team can use that as well to do the distribution of these questions for us.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Can I make one suggestion? At the tiger team hearing that we had on consent, Paul, I don't think you were there, but we had heard about different ways of getting consent from consumers, and we had made a request to those organizations to share with us the consent forms that they use. I'm sure not everybody would like to read those, but I think it's very instructive to look at actual consent forms for these kinds of discussions. So if we could get those, I certainly would be interested.

Paul Egerman – eScription – CEO

Sounds great. Let's see if we can do that for you. Before we open up for public comment, are there any other comments? Let me just say, this has been a terrific meeting. We got through the remaining six questions. We got started on the consent discussion. This is huge progress. I want to thank all the tiger team members. This has been really truly excellent. I know this is a long three-hour meeting, and I know it's a lot of work, and I very much appreciate your dedication. Judy Sparrow, can we open the phones up for public comments?

Judy Sparrow – Office of the National Coordinator – Executive Director
Very good call. Operator, can we see if we have any public comment, please?

Operator
Ms. Pam Jodock, you may speak, and identify yourself, please.

Pam Jodock – WellPoint – Issues Management Director
Thank you. This is Pam Jodock. I'm with WellPoint. I have a comment, and I also had several questions, so I guess my first question is, is there a limit to how many questions I'm allowed to ask?

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, you have a three-minute limit, and if you have further questions, you can e-mail me, and I'll distribute to the workgroup.

Pam Jodock – WellPoint – Issues Management Director
My first comment is, at the beginning of this call, as you were focused on question four regarding limiting provider exchange, it might be helpful for the group to know that in the HHS proposed rules that were issued on July 8th for privacy and security, HIOs would become a covered entity, as would RHIOs, regional health information exchanges, and e-prescribing entities.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Business associates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Pam Jodock – WellPoint – Issues Management Director
Business associates is still open, but they would be considered covered entities would be directly … directly applicable to them. Some of the conversation earlier suggested that that wasn't happening, but … that. And then the discussions in the first set of questions that you discussed, the one through nine questions were focusing mostly on health information organizations. I wondered if the group might want to consider applying those same questions to any organization that's engaged in electronic exchange on behalf of multiple participants such as regional health information, organizations, large hospital systems, and maybe what some states are now referring to as qualified organizations who are going to be providing the on ramp to the state HIO for individual providers. That's food for thought.

I had a question, and I apologize that I don't know all of the individuals who participate for tiger team, but I think Carol made a comment about HIOs collecting public health information, and I was curious. There are entities. There are third parties who collect public health information today, and I wondered why Carol thought that an HIO would act any differently than those entities today do in collecting that information. You made a comment that HIOs could collect any information they wanted to get the minimum necessary, and I was curious about your thought process behind that.

Judy Sparrow – Office of the National Coordinator – Executive Director
I think the purpose here is just for you to make a comment. It's not necessary that any of the workgroup members respond to a direct question, but duly noted. Any other comments?

Paul Egerman – eScription – CEO
Thank you very much, Pam, for those comments. Very helpful.

Judy Sparrow – Office of the National Coordinator – Executive Director
Any other public comments?

Operator
Yes, we have the next one from Ms. Looney. Please proceed.

Kristin Looney – Regenstrief
Hello. My name is Kristin Looney from the Regenstrief Institute, and I was just going to ask that, like some of the documents today weren't … for download, and so it makes it difficult to follow so that we can participate. And also, some of the most recent meetings have not been the audio from the meeting has not been posted on the Web site, so if those things could be posted, it would make it easier for those of trying to track everything to be involved.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Any other comments?

Operator
Ms. Francis, please proceed. Leslie Francis, your line is open.

W
Check your mute button, please.

Operator
From the University of Utah, Leslie Francis.

Judy Sparrow – Office of the National Coordinator – Executive Director
She must have hung up. Anyone else? Last call.

Operator
No, that was it.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. I'll turn it back to Paul

Paul Egerman – eScription – CEO
Thank you very much, Judy Sparrow, for all of your help in putting together our meetings, and thank you to Joy Pritts, and certainly thank you to the entire team from MITRE. Lisa and Linda are doing terrific jobs. And thanks again to the tiger team members. Our next meeting is Friday at 10:00.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

Paul Egerman – eScription – CEO

Take care.

Judy Sparrow – Office of the National Coordinator – Executive Director
Bye-bye.

Public Comment Received During the Meeting

1. Task Regarding Question #4 it may be helpful for the group to know that proposed privacy & security rules released by HHS for comment last week would make HIOs a HIPAA covered entity.

3. Re: Question #4, there are 3rd party entities in operation today that collect PHI for the purpose of public health reporting. Why does Carol think that an HIO would behave differently in fulfilling this role than those entities do today, e.g. why does she think an HIO would collect more information than necessary to achieve the "minimum necessary" required for the purpose of public reporting?